11a/b/g Outdoor Wireless Multi-Client Bridge/AP

User's Manual

Version: 1.0

Table of Contents

1 INTRODUCTION 5

1.1 FEATURES & BENEFITS 5
1.2 PACKAGE CONTENTS 6
1.3 BRIDGE/AP DESCRIPTION 6
1.4 SYSTEM REQUIREMENTS 6
1.5 APPLICATIONS 7
1.6 NETWORK CONFIGURATION 7
a) Ad-hoc (peer-to-peer) Mode 7
b) Infrastructure Mode 8

2 UNDERSTANDING THE HARDWARE 9

2.1 HARDWARE INSTALLATION 9
2.2 IP ADDRESS CONFIGURATION 9

3 CLIENT BRIDGE MODE – WEB CONFIGURATION 11

3.1 LOGGING IN 11
3.2 SYSTEM 13
3.2.1 ADMINISTRATOR SETTINGS 13
3.2.1.1 SAVE CONFIGURATION TO A FILE 15
3.2.1.2 RESTORE THE CONFIGURATION FROM A FILE 15
3.2.2 ADVANCED WIRELESS SETTINGS 16
3.2.3 FIRMWARE UPGRADE 17
3.2.4 SYSTEM REBOOT AND RESTORE SETTINGS TO DEFAULT 18
3.2.4.1 SYSTEM REBOOT 18
3.2.4.2 RESTORE SETTINGS TO DEFAULT 19
3.2.5 SYSTEM TIME CONFIGURATION 19
3.3 WIRELESS 21
3.3.1 NUMBER OF ACCESS POINTS 21
3.3.2 WIRELESS 11A & 11B/G CONFIGURATION 22
3.3.3 INFRASTRUCTURE / AD-HOC MODE 22
3.3.4 WIRELESS SECURITY 23
3.3.4.1.1 WEP (WIRED EQUIVALENT PRIVACY) 23
3.3.4.1.2 WPA – PERSONAL (WI-FI PROTECTED ACCESS) 25
3.4 LAN SETTINGS (STATIC / DHCP) 26
3.5 LOGS 27
3.6 STATISTICS 28

4 ACCESS POINT MODE – WEB CONFIGURATION 29

4.1 LOGGING IN 29
4.2 SYSTEM 30
4.2.1 ADMINISTRATOR SETTINGS 30
4.2.1.1 SAVE CONFIGURATION TO A FILE 30
4.2.1.2 RESTORE THE CONFIGURATION FROM A FILE 31
4.2.2 ADVANCED WIRELESS AND WDS 32
4.2.3 FIRMWARE UPGRADE 33
4.2.4 SYSTEM REBOOT AND RESTORE SETTINGS TO DEFAULT 34
4.2.4.1 SYSTEM REBOOT 34
4.2.4.2 RESTORE SETTINGS TO DEFAULT 35
4.2.5 SYSTEM TIME CONFIGURATION 36
4.2.6 WIZARD 37
4.2.6.1 CONNECTION SETUP WIZARD 37
4.2.6.2 WIRELESS SECURITY SETUP WIZARD 39
4.2.6.2.1 WIRELESS SECURITY LEVEL: BEST 40
4.2.6.2.2 WIRELESS SECURITY LEVEL: BETTER 41

4.2.6.2.3 WIRELESS SECURITY LEVEL: GOOD 42
4.3 WIRELESS CONFIGURATION 43
4.3.1.1 WEP (WIRED EQUIVALENT PRIVACY) 43
4.3.1.2 WPA PERSONAL (WI-FI PROTECTED ACCESS) 44
4.3.1.3 WPA ENTERPRISE (WI-FI PROTECTED ACCESS & 802.1X) 45
4.4 LAN 47
4.5 DHCP SERVER 48
4.6 MAC ADDRESS FILTER 50
4.7 LOGS 51
4.8 STATISTICS 52

APPENDIX A – SPECIFICATIONS 53

APPENDIX B – FCC INTERFERENCE STATEMENT 54

Revision History

Version	Date	Notes
1.0	June 4, 2006	Initial Version

1 Introduction

The Wireless High Power and High Gain Multi-Client Bridge/Access Point/ WDS (wireless distribution system) operates seamlessly in the dual band 2.4/5 GHz frequency spectrum supporting the 802.11b (2.4GHz, 11Mbps) and the newer, faster 802.11g (2.4GHz, 54Mbps)/ 802.11a (5GHz, 54Mbps) wireless standards.

The High output power and high sensitivity can extend range and coverage to reduce the roaming between APs to get more stability wireless connection. It can collocate with any high gain antenna you want for your environment.

To protect your wireless connectivity, this device can encrypt all wireless transmissions through 64/128-bit WEP data encryption and also supports WPA2/WPA/802.1x for powerful security authentication. The MAC addresses filter lets you select exactly which stations should have access to your network.

This chapter describes the features & benefits, package contents, applications, and network configuration.

1.1 Features & Benefits

Features	Benefits
High Speed Data Rate Up to 54Mbps	Capable of handling heavy data payloads such as MPEG video streaming
High Output Power up to 26 dBm in 11b/g	Spreads the operation distance and reduce the roaming between APs to get more stability wireless connection
IEEE 802.11b/g Compliant	Fully Interoperable with IEEE 802.11b/IEEE802.11g compliant devices
Point-to-point, Point-to-multipoint Wireless Connectivity	Let users transfer data between two buildings or multiple buildings
WPA2/WPA/ IEEE 802.1x support	Powerful data security
Hide SSID (AP Mode)	Avoids unallowable users sharing bandwidth, increases efficiency of the network
DHCP Client/ Server	Simplifies network administration
WDS (Wireless Distributed System)	Make wireless AP and Bridge mode simultaneously as a wireless repeater
MAC address filtering (AP Mode)	Ensures secure network connection
SNMP/Telnet Remote Configuration Management	Help administrators to remotely configure or manage the Access Point easily.
Watertight and Weatherproof	Avoid water invaded and weather corroded
Power-over-Ethernet (IEEE802.3af Compliant)	Flexible Access Point locations and cost savings

1.2 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped in its original package.

- Outdoor Wireless Client Bridge unit
- 48V, 0.375A AC/DC adapter with wall-plug power code
- One Dual Band SMA Antenna.
- Inline Power Injector (PoE)
- 1.8m Grounding Cable
- User manual CD-disc
- Wall mounting kit
- Mast mounting kit

1.3 Bridge/AP Description

1.4 System Requirements

The following are the minimum system requirements in order configure the device.

- PC/AT compatible computer with a Ethernet interface.
- Operating system that supports HTTP web-browser

1.5 Applications

The wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

a) **Difficult-to-wire environments**
   There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.
b) **Temporary workgroups**
   Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.
c) **The ability to access real-time information**
   Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.
d) **Frequently changed environments**
   Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.
e) **Small Office and Home Office (SOHO) networks**
   SOHO users need a cost-effective, easy and quick installation of a small network.
f) **Wireless extensions to Ethernet networks**
   Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.
g) **Wired LAN backup**
   Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.
h) **Training/Educational facilities**
   Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

1.6 Network Configuration

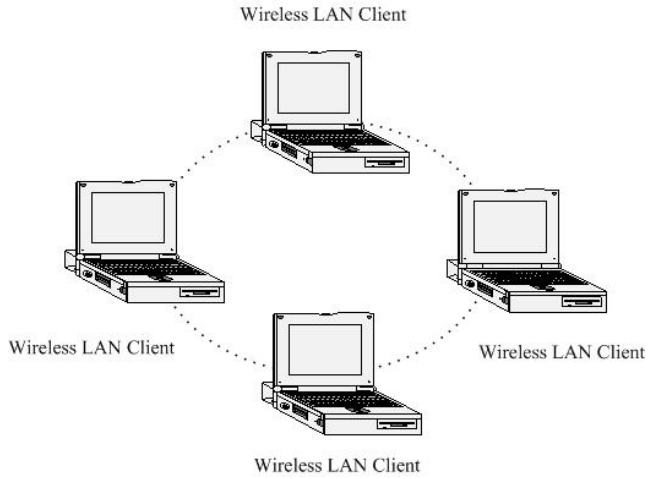
To better understand how the wireless LAN products work together to create a wireless network, it might be helpful to depict a few of the possible wireless LAN PC card network configurations. The wireless LAN products can be configured as:

a) Ad-hoc (or peer-to-peer) for departmental or SOHO LANs.
b) Infrastructure for enterprise LANs.

a) Ad-hoc (peer-to-peer) Mode

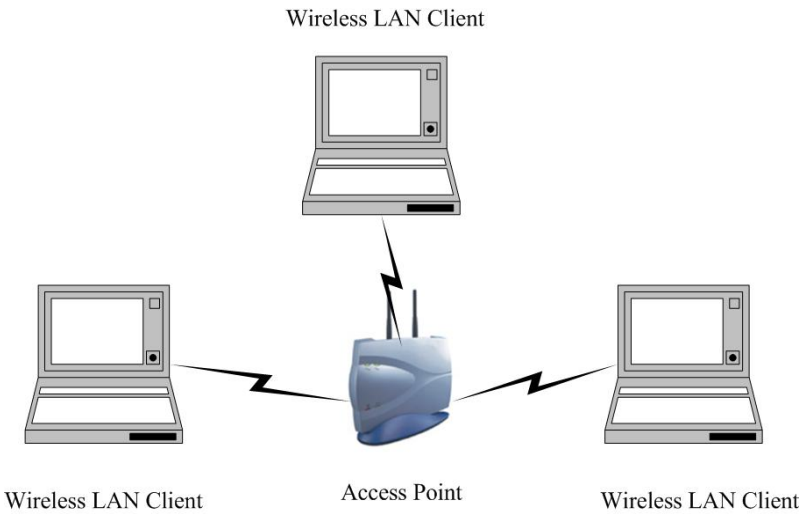
This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they

are within range of one another. In ad-hoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network. The image below depicts a network in ad-hoc mode.



b) Infrastructure Mode

The infrastructure mode requires the use of an access point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations. The image below depicts a network in infrastructure mode.

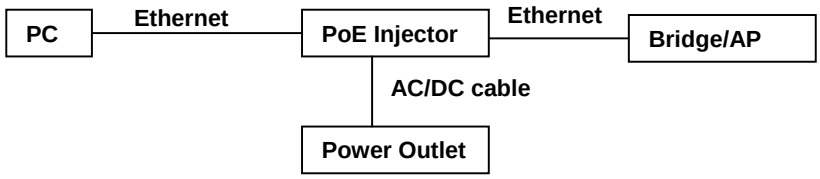


2 Understanding the Hardware

2.1 Hardware Installation

1. Place the unit in an appropriate place after conducting a site survey.
2. Plug one end of the Ethernet cable into the AP port of the PoE Injector and the other end into the Bridge/AP.
3. Place one end of another Ethernet cable into the Network port of the PoE Injector and another end into your PC/Notebook.
4. Insert the DC-inlet of the power adapter into the port labeled “DC-IN” and the other end into the power socket on the wall.

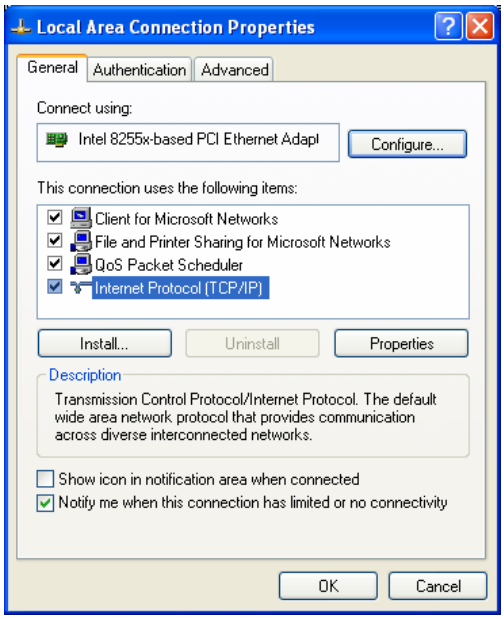
This diagram depicts the hardware configuration



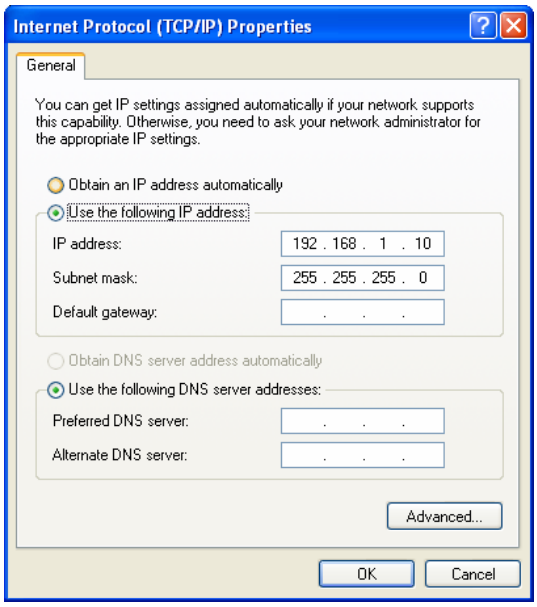
2.2 IP Address Configuration

This device can be configured as a Bridge/Router or Access Point. The default IP address of the device is **192.168.1.1 (Client Bridge mode)**, **192.168.1.2 (Access Point mode)**. In order to log into this device, you must first configure the TCP/IP settings of your PC/Notebook.

1. In the control panel, double click Network Connections and then double click on the connection of your Network Interface Card (NIC). You will then see the following screen.



2. Select **Internet Protocol (TCP/IP)** and then click on the **Properties** button. This will allow you to configure the TCP/IP settings of your PC/Notebook.



3. Select **Use the following IP Address** radio button and then enter the IP address and subnet mask. Ensure that the IP address and subnet mask are on the same subnet as the device.
   For Example: Device IP address: 192.168.1.1, 192.168.1.2
   PC IP address: 192.168.1.10
   PC subnet mask: 255.255.255.0

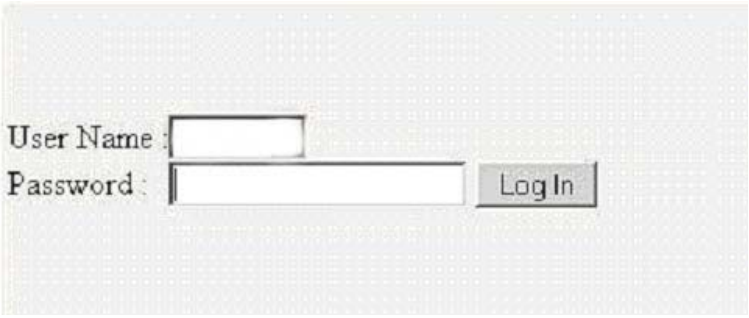
4. Click on the **OK** button to close this window, and once again to close LAN properties window.

3 Client Bridge Mode – Web Configuration

3.1 Logging In

- To configure the Bridge through the web-browser, enter the IP address of the Bridge (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.

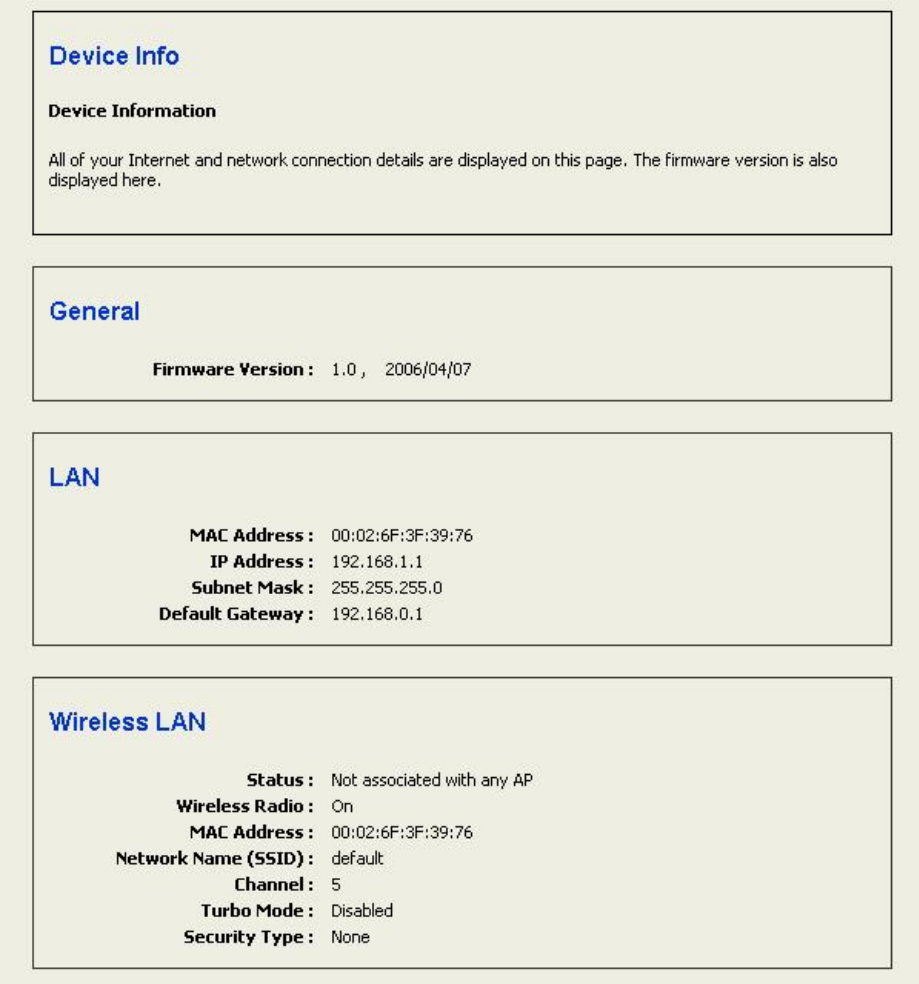
- Make sure that the Bridge and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page. Specify the **User Name** and **Password**. The device does not have a User Name and password configured by default, therefore please leave the password field blank and then click on the **Login** button.



- After logging in you will graphical user interface (GUI) of the bridge. The navigation drop-down menu on left is divided into six main sections:

1. **System**: This menu includes the administrator settings, advanced wireless settings such as wireless MAC clone and RTS/fragmentation threshold. Also included are other system related settings such as firmware upgrade, reset to factory defaults, and system date/time configuration.
2. **Wireless**: This menu includes the settings such as network type (infrastructure/ad-hoc), data rate, and security.
3. **LAN**: This menu includes the configuration of the LAN port and settings for the LAN IP, subnet mask, default gateway and DHCP client.
4. **Logs**: This menu displays a log of the critical and informational events that are triggered on the device.
5. **Statistics**: This menu displays the wired and wireless interface statistics.
6. **Help**: This menu describes the features of the device and the parameters for each setting.

- The Bridge status page is also displayed once you have logged in. This includes details about the system date and firmware, LAN IP address and MAC address and the wireless settings such as the radio status, MAC address, SSID, RF channel, and security.



- **General:**
  - Displays firmware version and system date.
- **LAN**:
  - Displays the MAC address, IP address, and subnet mask of the LAN interface.
- **Wireless LAN:**
  - Displays the status, MAC address, SSID, RF channel, and security settings of the wireless interface.

3.2 System

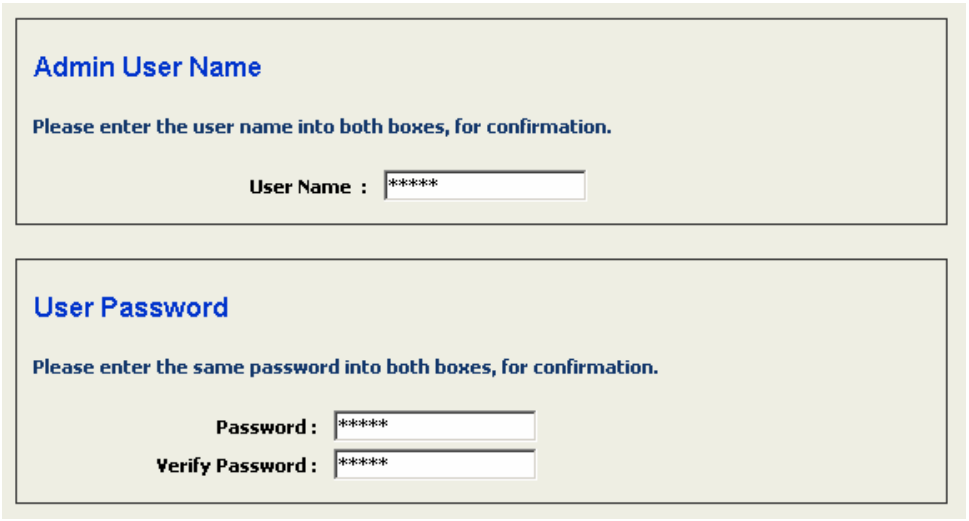
- Click on the **System** link on the navigation drop-down menu. You will then see five options: Administrators Settings, Advanced, Firmware, System, and Time. Each option is described below.

3.2.1 Administrator Settings

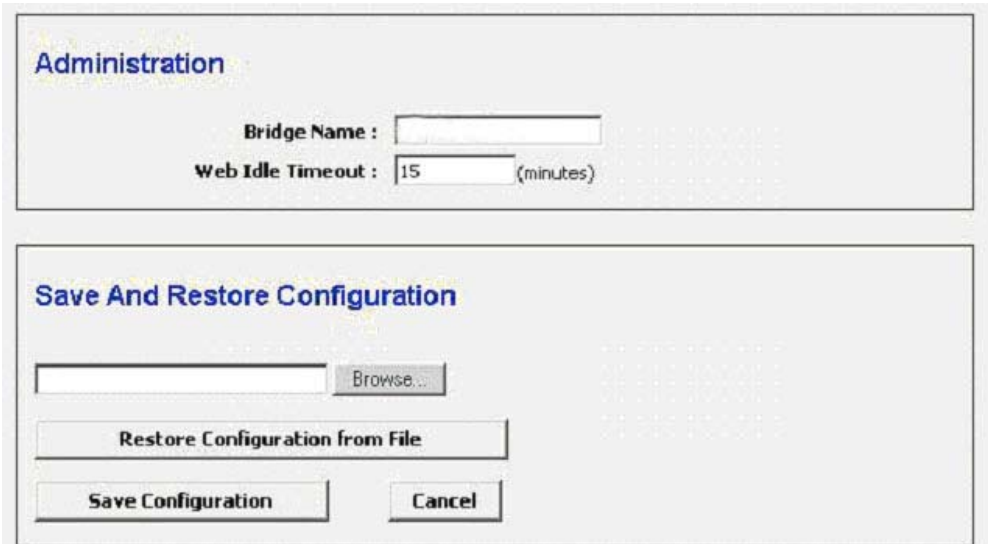
- Click on the **Administrator Settings** link under the **System** menu. This page allows you to configure the password to access this device from the web-browser. You can also specify a name for the bridge as well as backup and restore the system settings.

- The first part of this page gives you the option to save the changes that were made on this page. Click on the **Save Settings** button once you have configured the administrator settings.

- The second part of this page allows you to configure the user name and password for accessing the device. Specify a user name and password and then re-type it once again for verification. Click on the **Save Settings** button to store the changes.



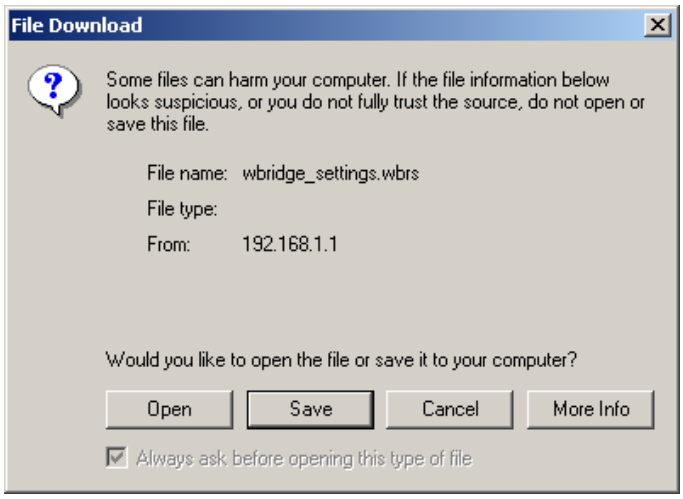
- The third part of this page allows you to specify a name for this device as well as save or restore a configuration Click on the **Save Settings** button to store the changes.



- **Bridge Name**: Specify a name for this bridge.
- **Web Idle Timeout**: Specify a time in minutes. If there is no activity on the configuration pages, then web page will close the session at the specified time.

3.2.1.1 Save Configuration to a File

- This option allows you to save the current configuration of the device into a file. Click on the **Save Configuration** button to begin.
- Save the file on your local disk by using the **Save** or **Save to Disk** button in the dialog box.



3.2.1.2 Restore the Configuration from a File

- This option allows you to restore a backup configuration from a file to the device. Click on the **Browse** button to select the file and then click on **Restore Configuration from a File** button.
- The system then prompts you to reboot the device.

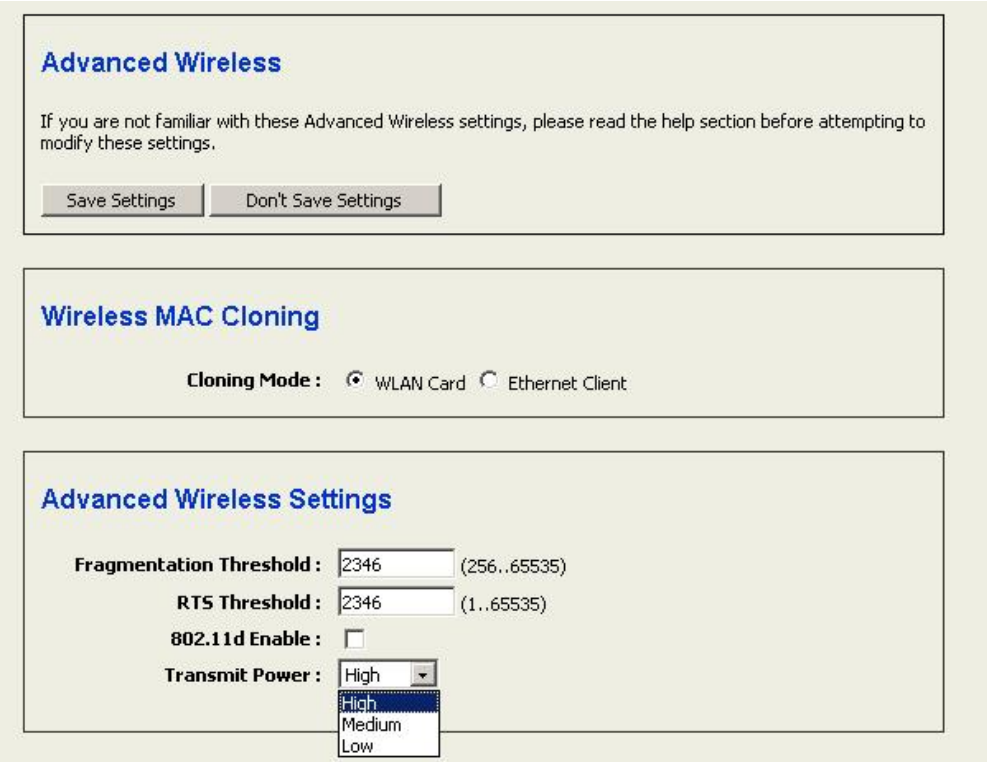
- Click on the **OK** button to continue. You will then see the **Rebooting** page.

- Please wait while the system is rebooting.

Note: Do no un-plug the device during this process as this may cause permanent damage.

3.2.2 Advanced Wireless Settings

- Click on the **Advanced** link under the **System** menu. This page allows you to enable wireless MAC cloning as well as configure the fragmentation threshold, RTS threshold, 802.11d, and the transmit power.



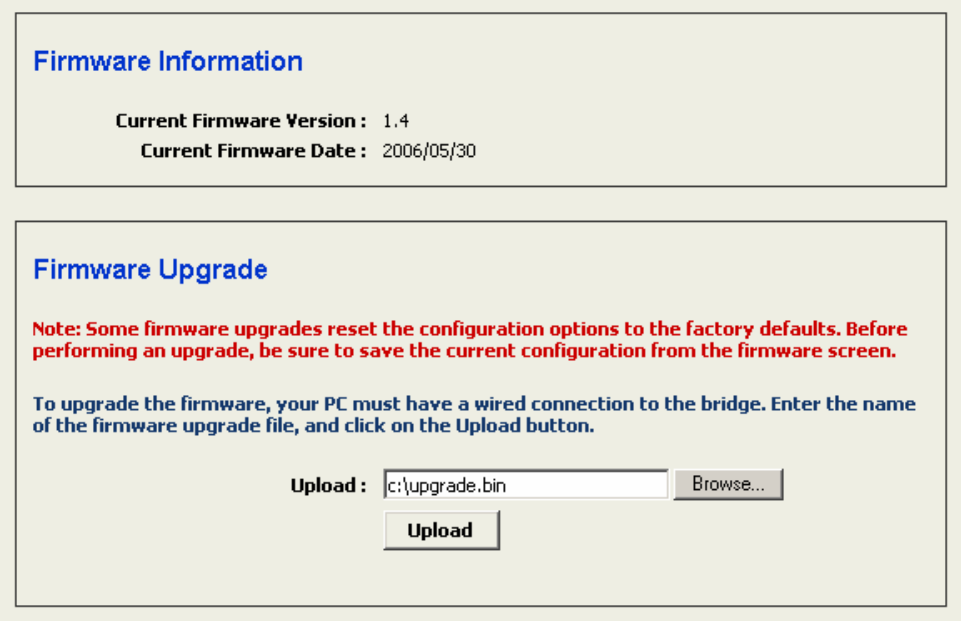
- **Bridge Name:** This feature controls the MAC address of the Bridge as seen by other devices (wired or wireless). If set to **Ethernet Client**, the MAC address from the first Ethernet client that transmits data through the Bridge will be used. This setting is useful when connected to an Xbox or if there is only one Ethernet device connected to the Bridge. When multiple Ethernet devices are connected to the Bridge, it may not be obvious which MAC address is being used. If set to **WLAN Card**, the MAC address of the WLAN card will be used. When multiple Ethernet devices are connected to the Bridge, the MAC address of the Bridge will not change.
- **Fragment Threshold**: Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 65535. The default value is 2346.
- **RTS Threshold**: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 1 and 65535. The default value is 2346.
- **802.11d Enable:** 802.11d is a wireless specification for operation in multiple regulatory domains. This supplement to the 802.11 specifications defines the physical layer requirements (channelization, hopping patterns, new values for current MIB attributes, and other requirements to extend the operation of 802.11 WLANs in multiple regulatory domains (countries). The current 802.11 standard defines operation in only a fixed regulatory domain (country). This supplement adds the requirements and definitions necessary to allow WLAN equipment to operate in

multiple markets. **Enable** this feature if you are traveling and operating in several regulatory domains. By default, this value is disabled.

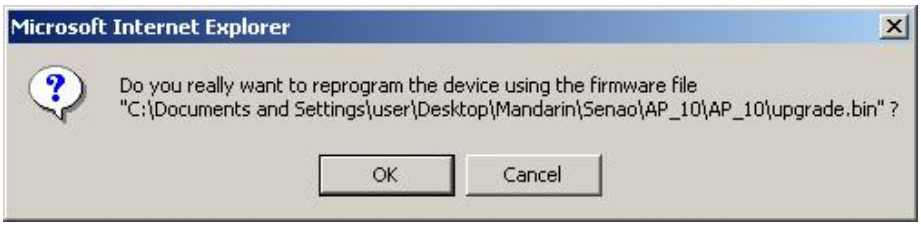
- **Transmit Power**: You may control the output power of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.
- Click on the **Save Settings** button once you have modified the settings.

3.2.3 Firmware Upgrade

- Click on the **Firmware** link under the **System** menu. This page allows you to upgrade the firmware of the device in order to improve the functionality and performance. This page also displays the current firmware version and its release date.



- Ensure that you have downloaded the appropriate firmware from the vendor's website. Connect the device to your PC using an Ethernet cable, as the firmware cannot be upgraded using the wireless interface.
- Click on the **Browse** button to select the firmware and then click on the **Upload** button.



- The above dialog box requests you to confirm the upgrade process. Click on the **OK** button to continue.
- Once you click on the **OK** button, you will return to the previous page which indicates that the upgrade process may take up to one minute.

- After a few seconds the firmware will start to re-program the device and you will see a countdown on the **Success** page.

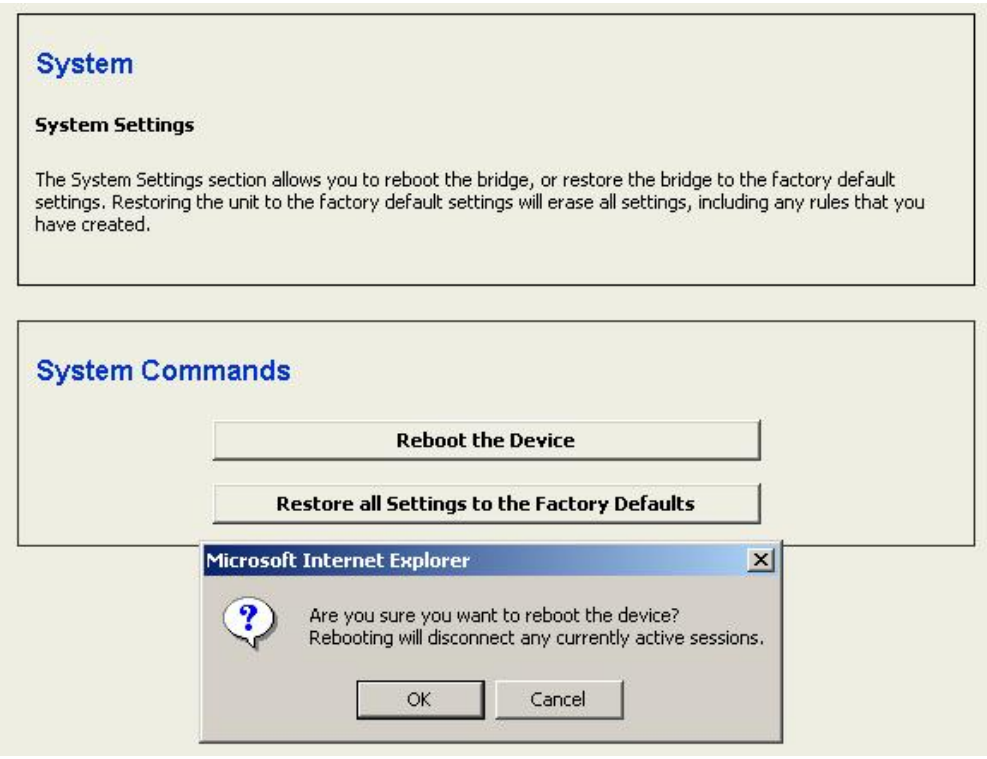
Note: Do not un-plug the device during this process. Some firmware upgrades may restore the configuration back to the factory default settings. Therefore you may need to restore a configuration from a file. Refer to **Administrator Settings** for details.

3.2.4 System Reboot and Restore Settings to Default

- Click on the **System** link under the **System** menu. This page allows you to reboot the device using the current settings or restore all the settings to the factory defaults.

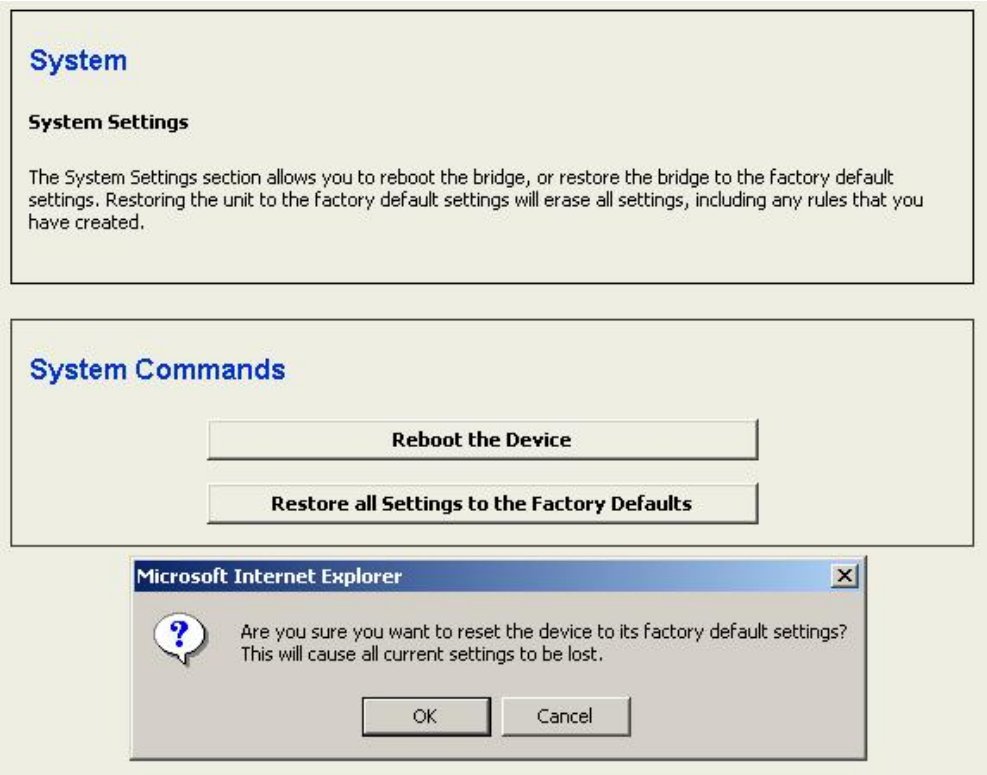
3.2.4.1 System Reboot

- Click on the **Reboot the Device** button to reboot the device using its current settings. Once the dialog box appears, click on the **OK** button to confirm the action.



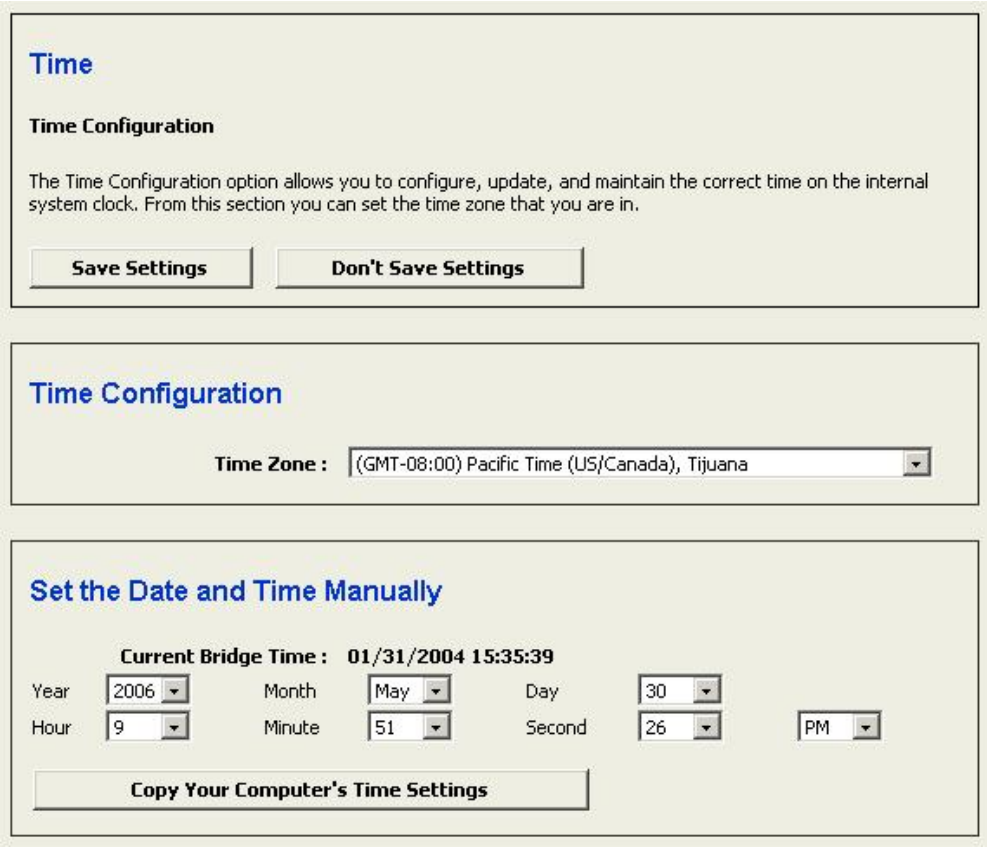
3.2.4.2 Restore Settings to Default

- Click on the **Restore all Settings to Factory Defaults** button. This option restores al configuration settings back to the settings that were in effect at the time when the device was shipped from the factory. Once the dialog box appears, click on the **OK** button to confirm the action.
  Note: The current settings will be lost.



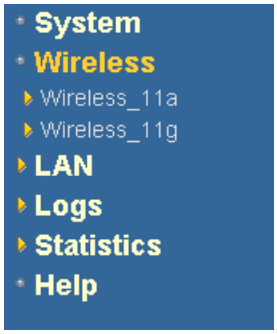
3.2.5 System Time Configuration

- Click on the **Time** link under the **System** menu. This feature allows you to configure, update, and maintain the correct time on the device's internal system clock as well as configure the time zone. The date and time of the device can be configured manually or by copying the time on the PC that it is wired to.
  Note: If the bridge losses power for any reason, it will not be able to keep its clock running, and will not display the correct time once the device has been restarted. Therefore, you must re-enter the correct date and time.



- **Time Zone**: Select your time zone from the drop-down list.
- **Set the Date and Time**: Select a date and time from the drop-down list or do to use computer's time and date click on the **Copy Your Computer's Time Settings** button.
- Click on the **Save Settings** button once you have modified the settings.

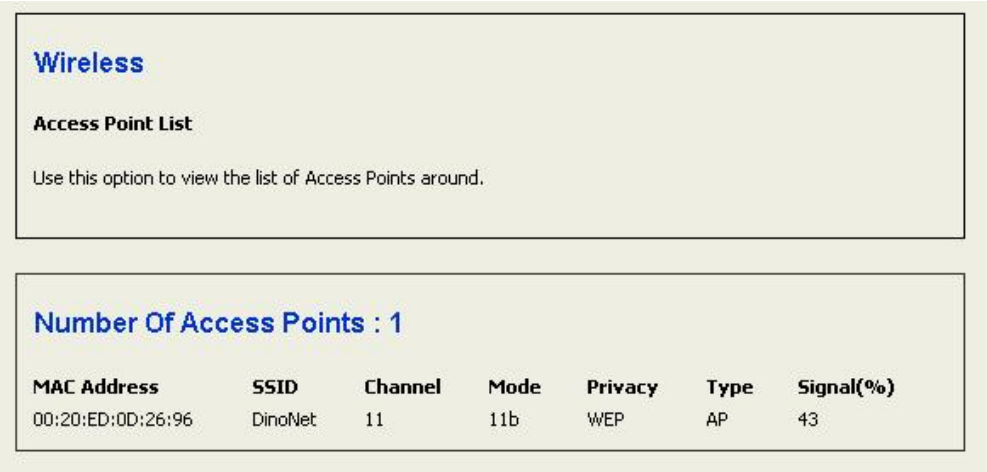
3.3 Wireless



- Click on the **Wireless** link on the navigation drop-down menu. You will then see two options: Wireless_11a and Wireless_11g. The configuration steps are the same for both radios.

3.3.1 Number of Access Points

- Click on the **Wireless** menu. This status page is like a site survey and displays a list of Access Points in the area.



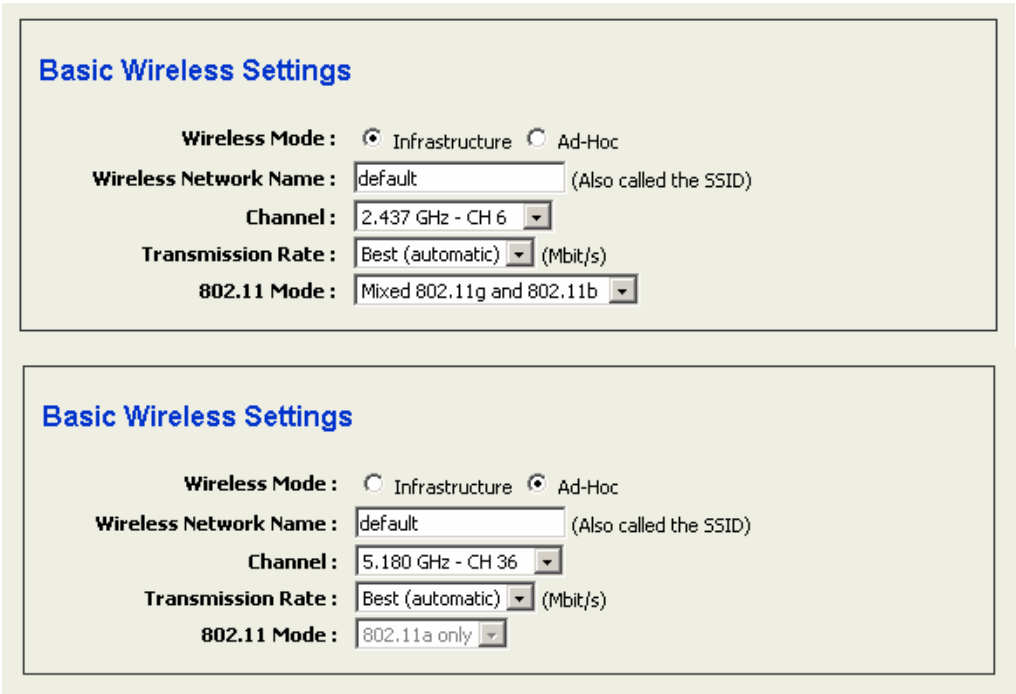
- **MAC Address**: The MAC address or BSSID of the Access Point.
- **SSID**: The name used to identify the wireless network. The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters.
- **Channel**: The channel used to communicate on the wireless network.
- **Mode**: Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
- **Privacy**: The type of security used on this network. It may be disabled, WEP, WPA, etc.
- **Type**: Wireless configuration mode such as Ad-Hoc or AP.
- **Signal (%)**: The wireless signal strength. Signal quality can be reduced by distance, by interference from other radio frequency devices and obstruction from obstacles between the bridge and AP.

3.3.2 Wireless 11a & 11b/g Configuration

- Click on the **Wireless_Setting** link under the **Wireless** menu. The first part of this page allows you to save the configuration. Click on the **Save Settings** button once you have modified the settings.

3.3.3 Infrastructure / Ad-hoc Mode

- Click on the **Wireless_Setting** link under the **Wireless** menu. The second part of this page allows you to configure the device in infrastructure or ad-hoc mode.



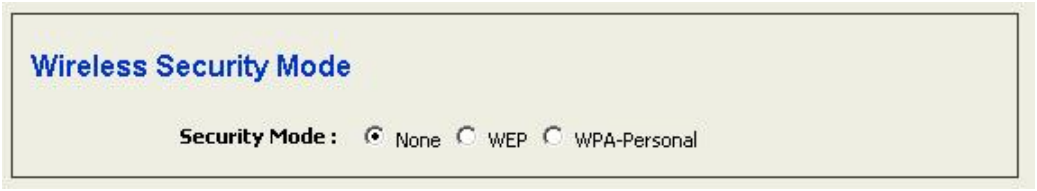
- **Wireless Mode:** Select the **Infrastructure** or **Ad-Hoc** radio button. Infrastructure is a point-to-multipoint (PtMp) topology where as Adhoc is a point-to-point topology (PtP).
- **Wireless Network Name**: The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters.
- **Channel**: Select a channel from the drop-down list. The channels available are based on the country's regulation. When selecting Infrastructure mode, a channel is

not required, however, when selecting Adhoc mode, you must select the same channel on all points.

- **Transmission Rate**: Select a transmission rate from the drop-down list. It is recommended to use the **Best (automatic)** option.
- **802.11 Mode**: Select the IEEE 802.11 mode from the drop-down list. For example, if you are sure that the wireless network will be using only IEEE 802.11g clients, then it is recommended to select **802.11g** only instead of **Mixed 802.11g and 802.11b** which will reduce the performance of the wireless network. You may also select **802.11b** only or **802.11a only**. Do not use this option when configured at Ad-Hoc mode.
- Click on the **Save Settings** button once you have modified the settings.

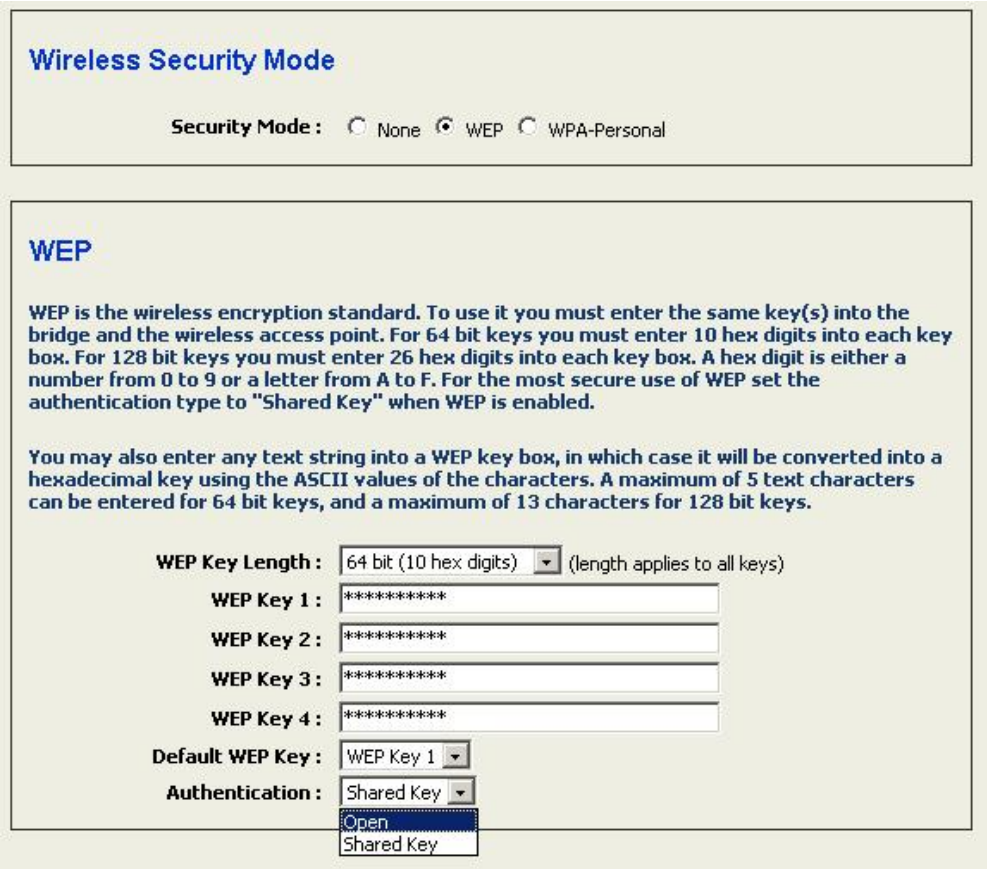
3.3.4 Wireless Security

- Click on the **Wireless_Setting** link under the **Wireless** menu. The third part of this page allows you to configure the security settings of this device. To protect your privacy this mode supports two types of wireless security: WEP and WPA-Personal. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server.
- Select the **None** radio button in order to disable security.



3.3.4.1.1 WEP (Wired Equivalent Privacy)

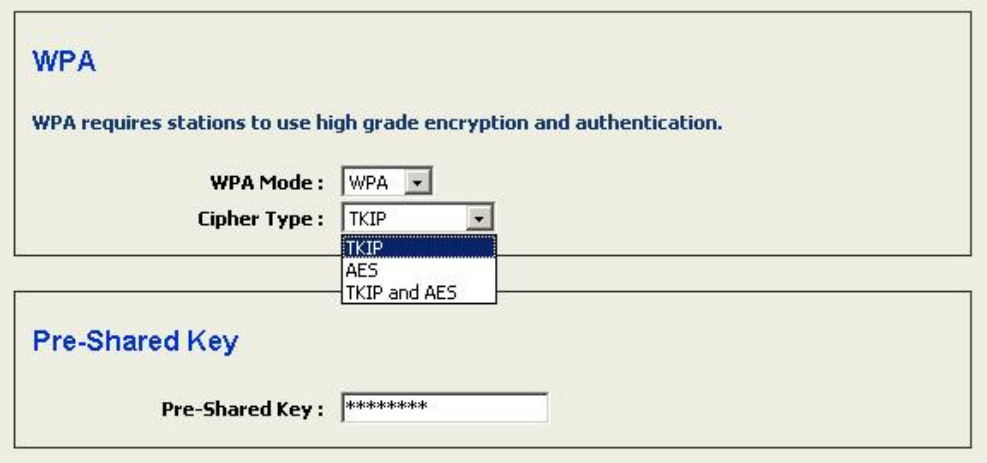
- Select the **WEP** radio button if your wireless network uses WEP encryption. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.
- WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.



- **WEP Key Length**: Select a **64-bit** or **128-bit** WEP key length from the drop-down list.
- **WEP Key 1-4:** You may enter four different WEP keys.
- **Default WEP Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- **Authentication:** Select **Open**, or **Shared Key**. Authentication method from the drop-down list. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.
- Click on the **Save Settings** button once you have modified the settings.

3.3.4.1.2 WPA – Personal (Wi-Fi Protected Access)

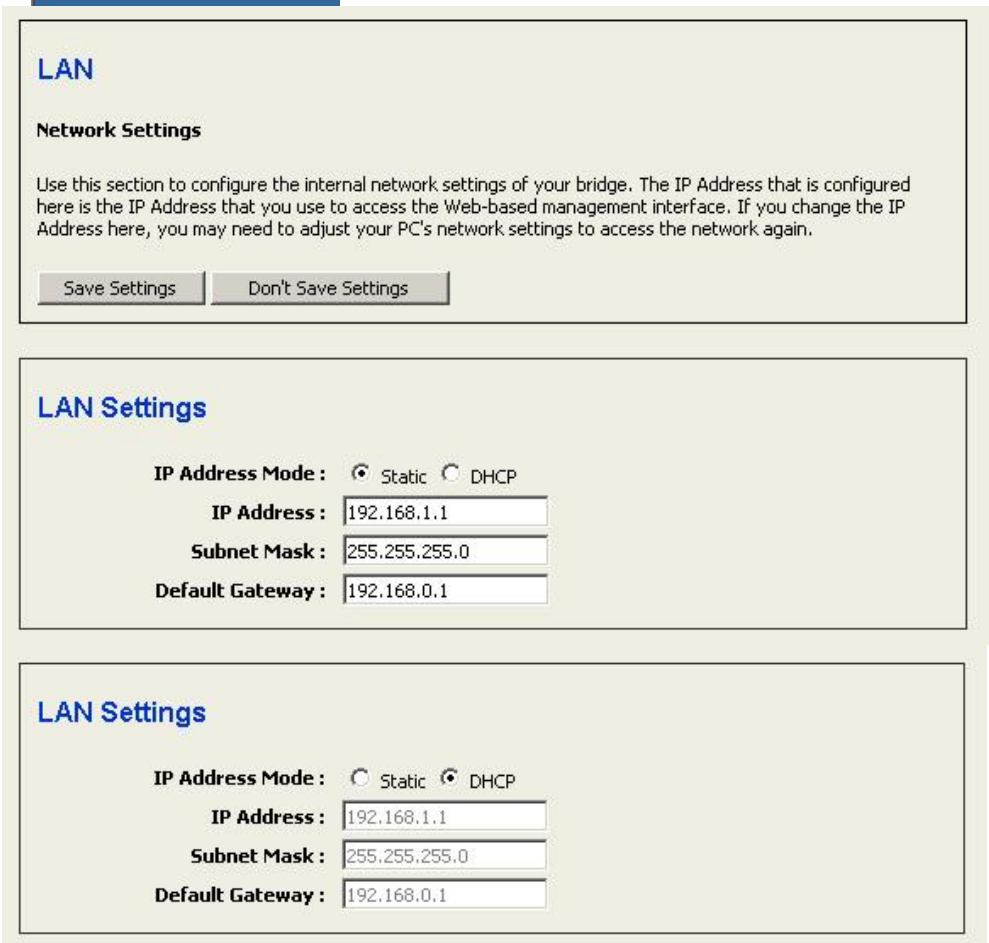
- Select the **WPA-Personal** radio button if your wireless network uses WPA encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.



- **WPA Mode**: Select the **WPA** from the drop-down list.
- **Cipher Type**: Select **TKIP** or **AES** as the cipher suite. The encryption algorithm used to secure the data communication. TKIP. Use TKIP only. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES. Use AES only. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES. TKIP and AES. The bridge negotiates the cipher type with the access point, and uses AES when available.
- **Pre-Shared Key:** The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.
- Click on the **Save Settings** button once you have modified the settings.

3.4 LAN Settings (Static / DHCP)

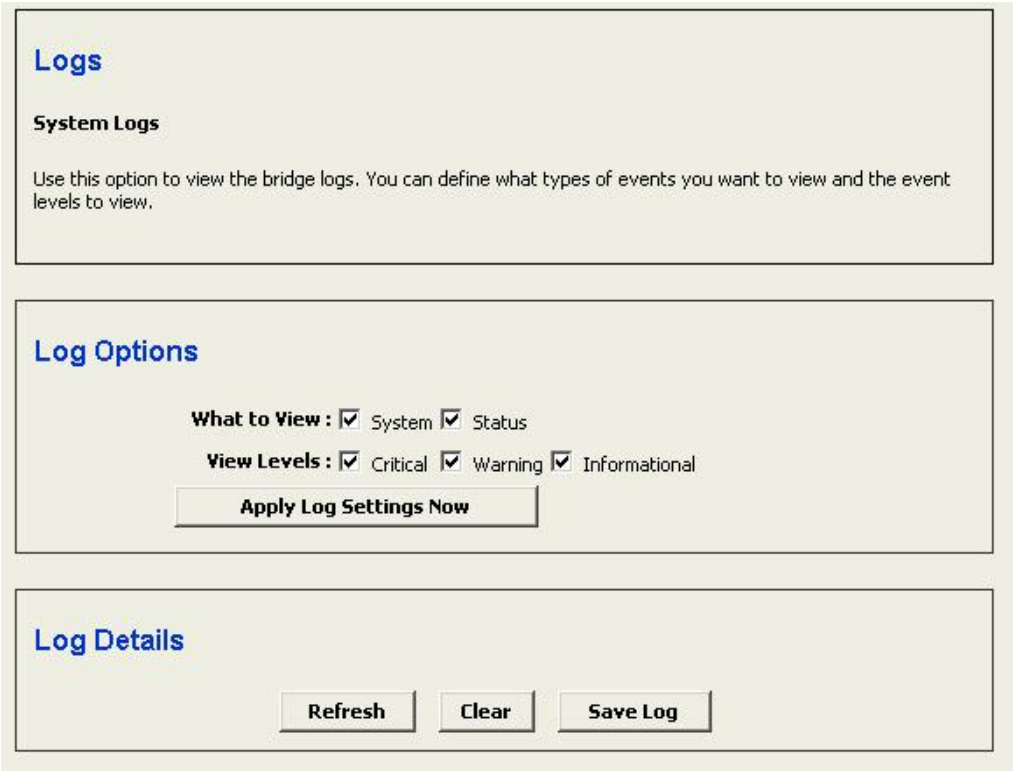
- Click on the **LAN** link on the navigation drop-down menu. This feature allows you to configure the LAN interface using a static IP address or as a DHCP client. This IP address is also used to access the web-based interface.



- **IP Address Mode:** Select the Static or DHCP radio button. If you select **DHCP** radio button, you are not required to enter the rest of the fields, as the IP address will be provided to the device by the AP or DHCP server. If you select the **Static** radio button, you must enter the IP address, subnet mask, and default gateway.
- **IP Address:** Enter an IP address for this device.
- **Subnet Mask:** Enter the subnet mask for this IP address.
- **Default Gateway:** Enter the IP address of the default gateway.
- Click on the **Save Settings** button once you have modified the settings.
  Note: If you change the IP address here, you may need to adjust your PC's network settings to access the network again.

3.5 Logs

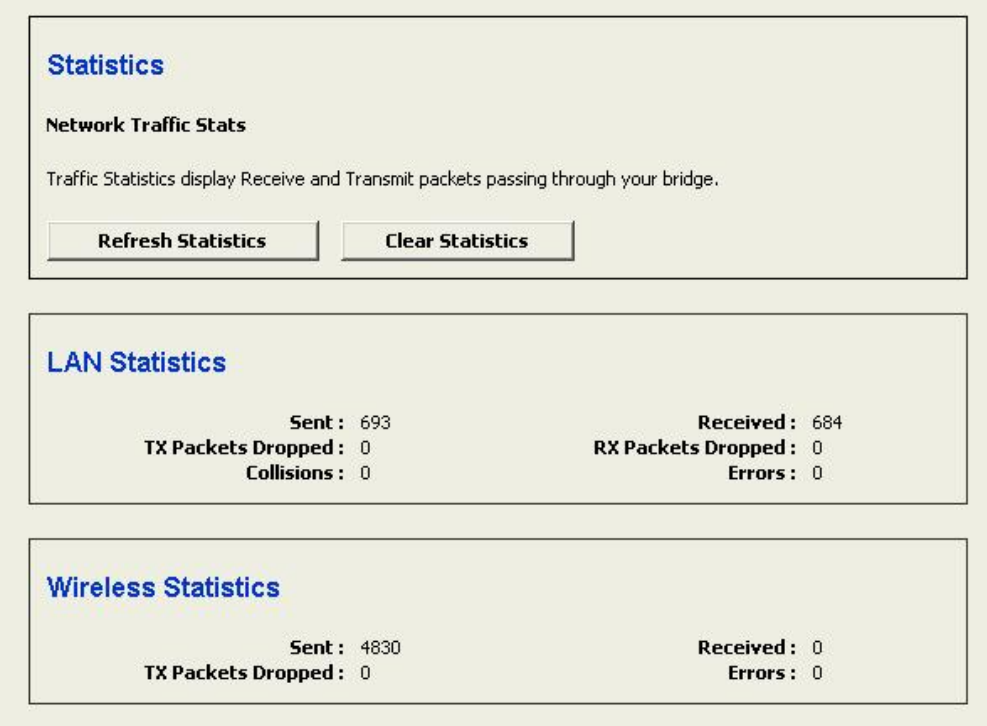
- Click on the **Logs** link on the navigation drop-down menu. Logs display a list of events that are triggered on the Ethernet and Wireless interface. This log can be referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.



- **Log Options:** Select the type of warning that you would like recorded and place a check in the appropriate box. Then click on the **Apply Log Settings Now** button.
- **Log Details**: The events are logged in this section. Click on the **Refresh** button to refresh the events or click on the **Clear** button to clear the events. Click on the **Save Log** button to save the log on your PC.

3.6 Statistics

- Click on the **Statistics** link on the navigation drop-down menu. This page displays the transmitted and received packet statistics of the wired and wireless interface.



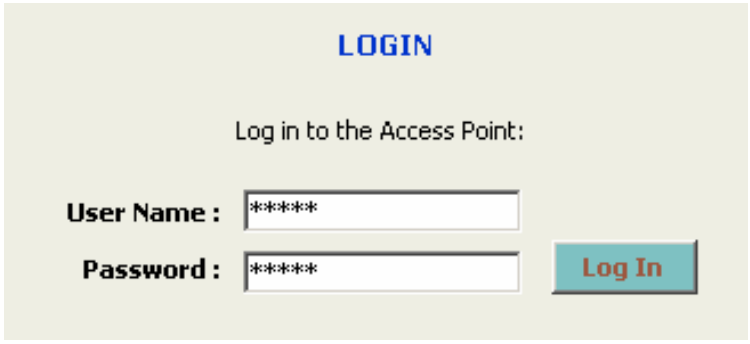
- **Sent**: The number of packets sent from the bridge.
- **Received**: The number of packets received by the bridge.
- **TX Packets Dropped**: The number of packets that were dropped while being sent, due to errors, collisions, or bridge resource limitations.
- **RX Packets Dropped**: The number of packets that were dropped while being received, due to errors, collisions, or bridge resource limitations.
- **Collisions**: The number of packets that were dropped due to Ethernet collisions (two or more devices attempting to use an Ethernet circuit at the same time).
- **Errors**: The number of transmission failures that cause loss of a packet. A noisy radio-frequency environment can cause a high error rate on the wireless LAN.
- Click on the **Refresh Statistics** button to refresh the events or click on the **Clear Statistics** button to clear the events.Bottom of Form

4 Access Point Mode – Web Configuration

4.1 Logging In

- To configure the Access Point through the web-browser, enter the IP address of the Access Point (default: **192.168.1.2**) into the address bar of the web-browser and press **Enter**.

- Make sure that the Bridge and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page. Specify the **User Name** and **Password**. The device does not have a User Name password configured by default, therefore please leave the password field blank and then click on the **Login** button.



- After logging in you will graphical user interface (GUI) of the Access Point. The navigation drop-down menu on left is divided into seven main sections:

1. **System**: This menu includes system related settings such as firmware upgrade, reset to factory defaults, system date/time configuration and configuration wizard.
2. **Wireless**:
3. **LAN**: This menu includes the LAN and DHCP client/server settings.
4. **Filter**: This menu includes MAC address filter and advanced wireless settings.
5. **Logs**: This menu displays the system log.
6. **Status**: This menu displays the wired and wireless statistics
7. **Help**: This menu describes the features of the device and the parameters for each setting.

4.2 System

- Click on the **System** link on the navigation drop-down menu. You will then see six options: Administrator Settings, Advanced, Firmware, System, Time, and Wizard. Each option is described below.

4.2.1 Administrator Settings

- Click on the **Administrator Settings** link under the **System** menu. This page allows you to configure the password to access this device from the web-browser. You can also backup and restore the system settings.

- Specify a user name and password and then re-type it once again for verification. Click on the **Save Settings** button to store the changes.

4.2.1.1 Save Configuration to a File

- This option allows you to save the current configuration of the device into a file. Click on the **Save Configuration** button to begin.
- Save the file on your local disk by using the **Save** or **Save to Disk** button in the dialog box.

4.2.1.2 Restore the Configuration from a File

- This option allows you to restore a backup configuration from a file to the device. Click on the **Browse** button to select the file and then click on **Restore Configuration from a File** button.
- The system then prompts you to reboot the device.

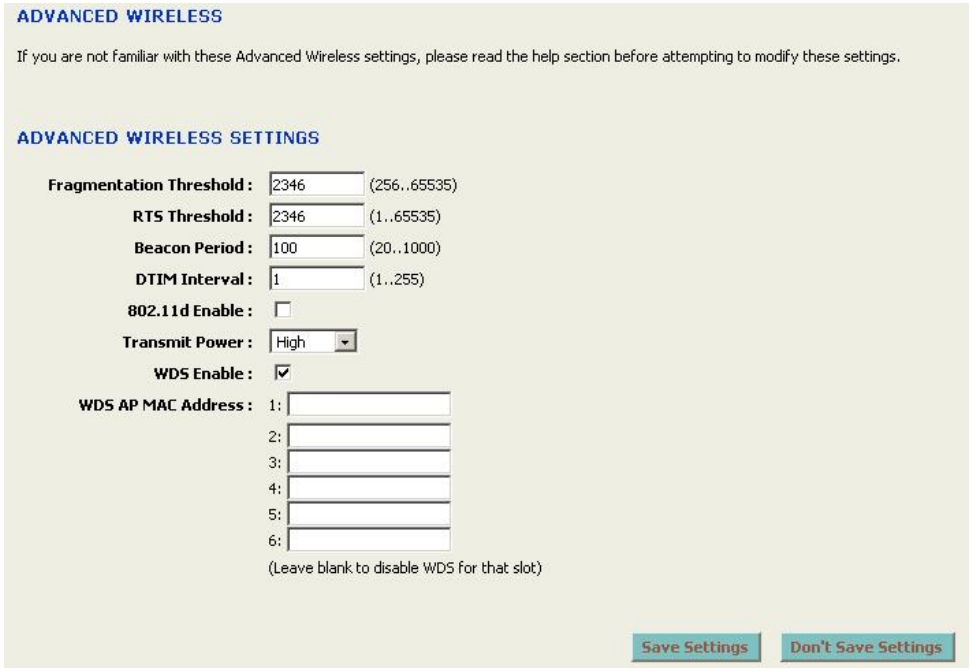
- Click on the **OK** button to continue. You will then see the **Rebooting** page.

- Please wait while the system is rebooting.

Note: Do no un-plug the device during this process as this may cause permanent damage.

4.2.2 Advanced Wireless and WDS

- Click on the **Advanced** link under the **System** menu. This page allows you to configure the fragmentation threshold, RTS threshold, 802.11d, transmit power and WDS (wireless distribution system).



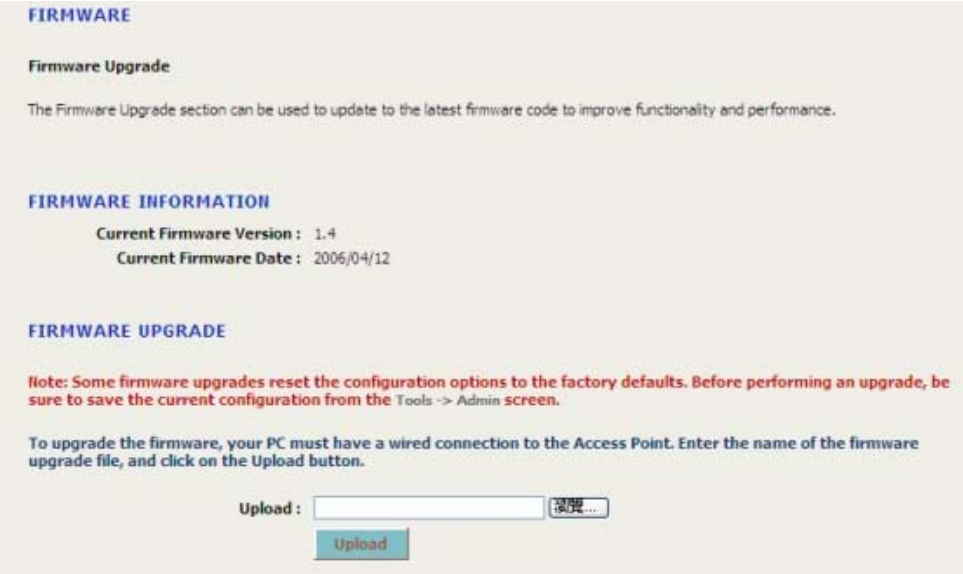
- **Fragment Threshold**: Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 65535. The default value is 2346.
- **RTS Threshold**: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 1 and 65535. The default value is 2346.
- **Beacon Period**: Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds.
- **DITM Interval**: A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.
- **802.11d Enable:** 802.11d is a wireless specification for operation in multiple regulatory domains. This supplement to the 802.11 specifications defines the physical layer requirements (channelization, hopping patterns, new values for current MIB attributes, and other requirements to extend the operation of 802.11 WLANs in multiple regulatory domains (countries). The current 802.11 standard defines operation in only a fixed regulatory domain (country). This supplement adds the requirements and definitions necessary to allow WLAN equipment to operate in

multiple markets. **Enable** this feature if you are traveling and operating in several regulatory domains. By default, this value is disabled.

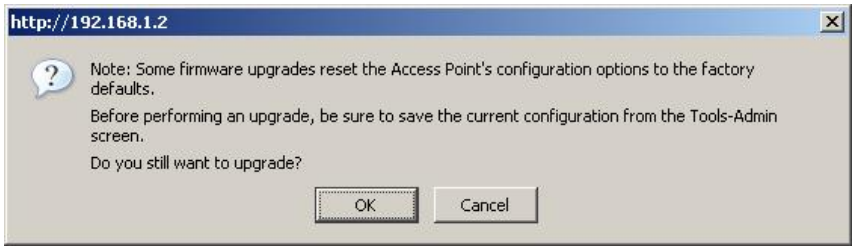
- **Transmit Power**: You may control the output power of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.
- **WDS**: Place a check in this box to enable WDS (Wireless Distribution System). When WDS is enabled, this access point functions as a wireless repeater and is able to wirelessly communicate with other APs via WDS links.
  Note that WDS is incompatible with WPA -- both features cannot be used at the same time. A WDS link is bidirectional; so this AP must know the MAC Address (creates the WDS link) of the other AP, and the other AP must have a WDS link back to this AP. Make sure the APs are configured with same channel number.
- **WDS AP MAC Address**: Specify one-half of the WDS link. The other AP must also have the MAC address of this AP to create the WDS link back to this AP.
- Click on the **Save Settings** button once you have modified the settings.

4.2.3 Firmware Upgrade

- Click on the **Firmware** link under the **System** menu. This page allows you to upgrade the firmware of the device in order to improve the functionality and performance. This page also displays the current firmware version and its release date.



- Ensure that you have downloaded the appropriate firmware from the vendor's website. Connect the device to your PC using an Ethernet cable, as the firmware cannot be upgraded using the wireless interface.
- Click on the **Browse** button to select the firmware and then click on the **Upload** button.



- The above dialog box requests you to confirm the upgrade process. Click on the **OK** button to continue.
- Once you click on the **OK** button, you will return to the previous page which indicates that the upgrade process may take up to one minute.

- After a few seconds the firmware will start to re-program the device and you will see a countdown on the **Success** page.

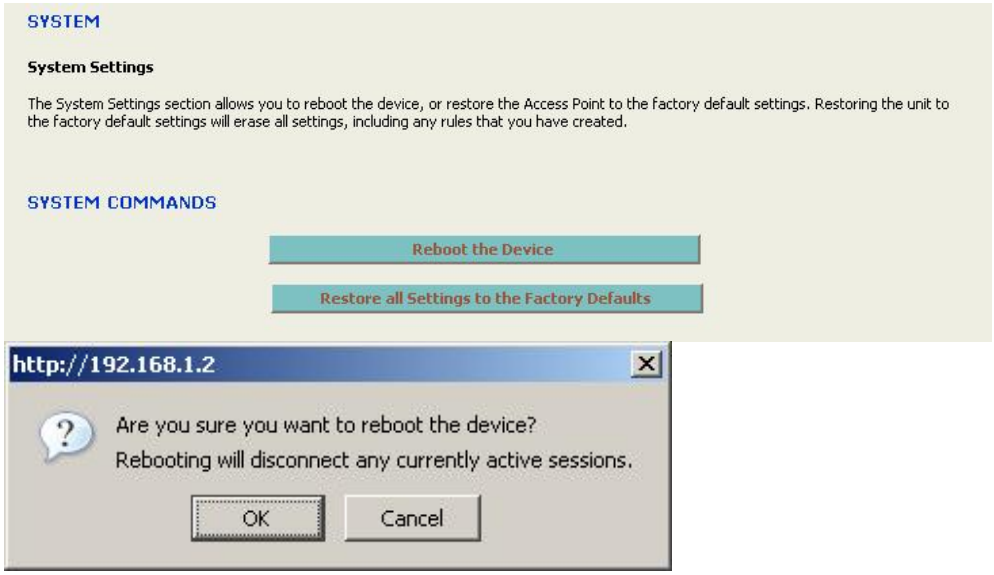
Note: Do not un-plug the device during this process. Some firmware upgrades may restore the configuration back to the factory default settings. Therefore you may need to restore a configuration from a file. Refer to **Administrator Settings** for details.

4.2.4 System Reboot and Restore Settings to Default

- Click on the **System** link under the **System** menu. This page allows you to reboot the device using the current settings or restore all the settings to the factory defaults.

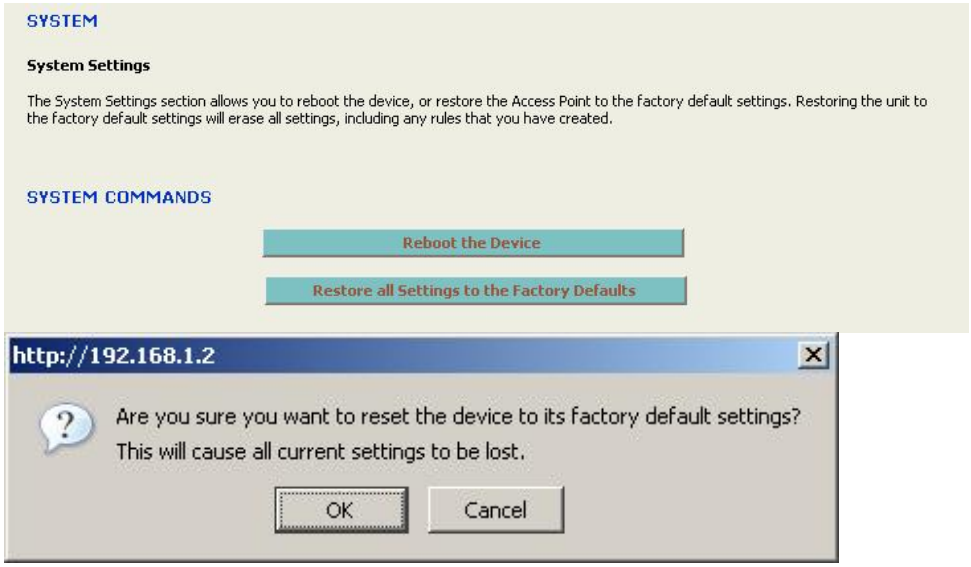
4.2.4.1 System Reboot

- Click on the **Reboot the Device** button to reboot the device using its current settings. Once the dialog box appears, click on the **OK** button to confirm the action.



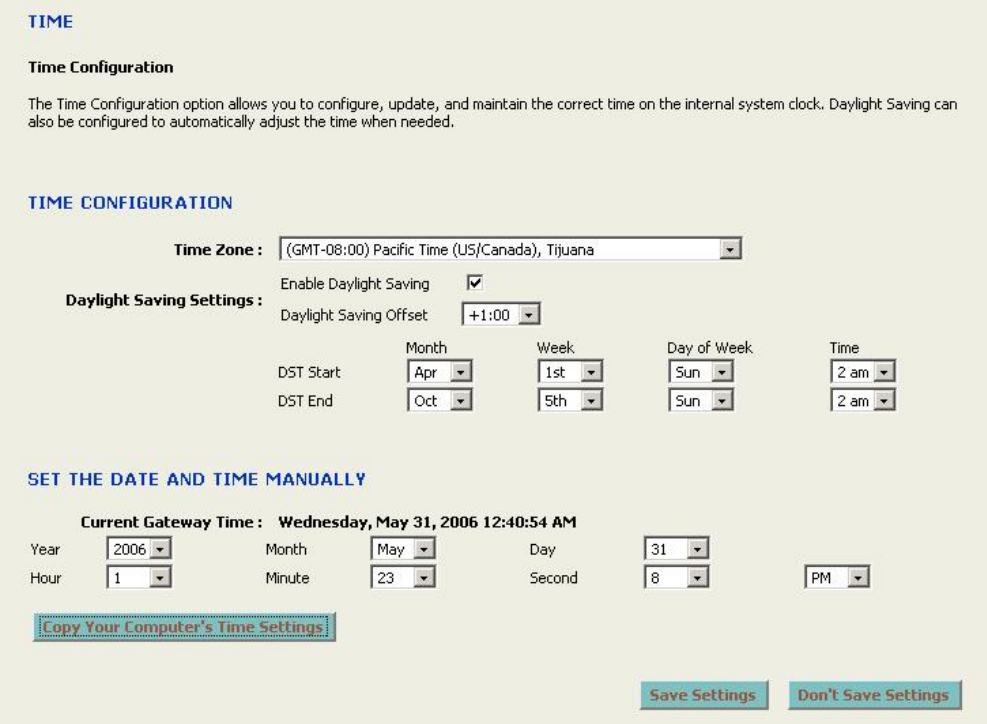
4.2.4.2 Restore Settings to Default

- Click on the **Restore all Settings to Factory Defaults** button. This option restores al configuration settings back to the settings that were in effect at the time when the device was shipped from the factory. Once the dialog box appears, click on the **OK** button to confirm the action.
  Note: The current settings will be lost.



4.2.5 System Time Configuration

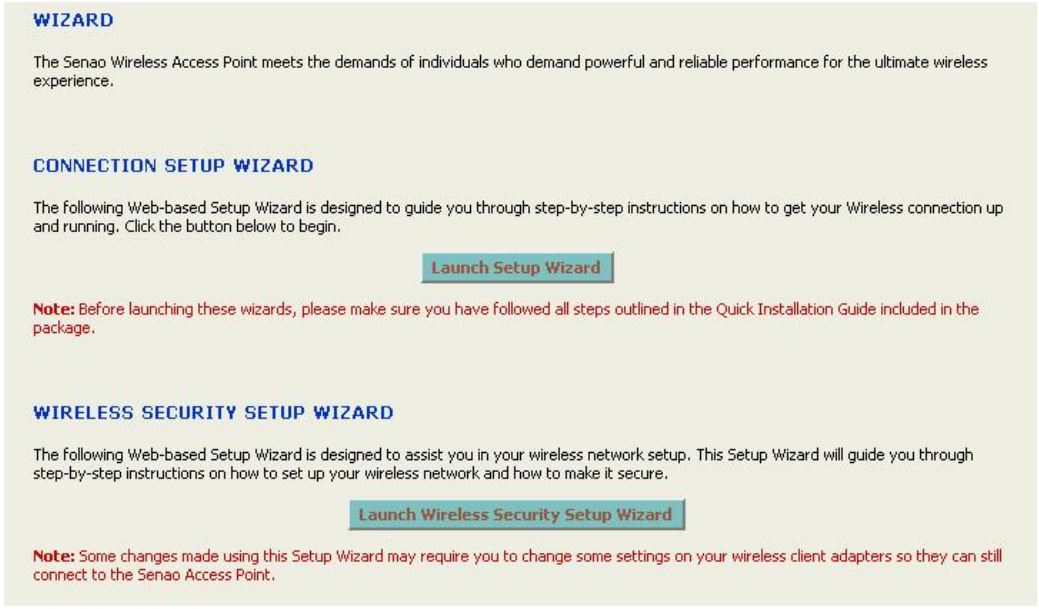
- Click on the **Time** link under the **System** menu. This feature allows you to configure, update, and maintain the correct time on the device's internal system clock as well as configure the time zone. The date and time of the device can be configured manually or by copying the time on the PC that it is wired to.
  Note: If the device losses power for any reason, it will not be able to keep its clock running, and will not display the correct time once the device has been restarted. Therefore, you must re-enter the correct date and time.



- **Time Zone**: Select your time zone from the drop-down list.
- **Set the Date and Time**: Select a date and time from the drop-down list or do to use computer's time and date click on the **Copy Your Computer's Time Settings** button.
- Click on the **Save Settings** button once you have modified the settings.

4.2.6 Wizard

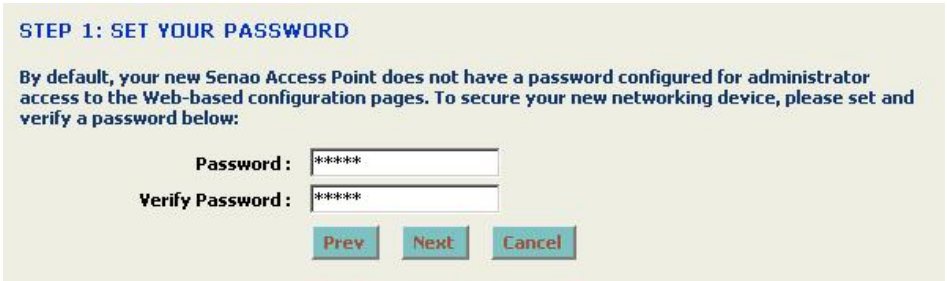
- Click on the **Wizard** link under the **System** menu. This wizard guides you in through the process of configuring the connection and security features of the Access Point.



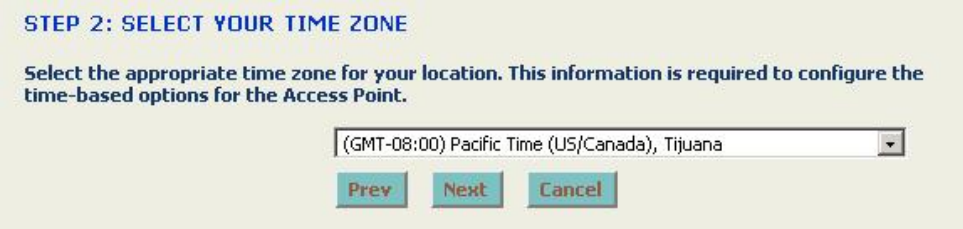
4.2.6.1 Connection Setup Wizard

- The connection wizard will guide you through the steps to get your network connection up and running.
- Click on the **Launch Setup Wizard** button.

- Click on the **Next** button to continue.

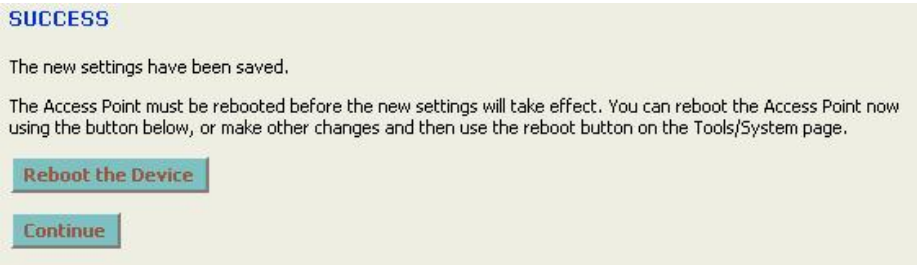


- By default, the Access Point does not have a password configured for administrator access to the web-based interface. Specify and password and then re-type it in the verification box. Then click on the **Next** button.



- Select your time zone from the drop-down list and then click on the **Next** button.

- The setup wizard is almost complete, click on the **Connect** button.



- The configuration has been saved, click on the **Reboot the Device** button.

- The dialog box asks you to confirm your action, click on the **OK** button.

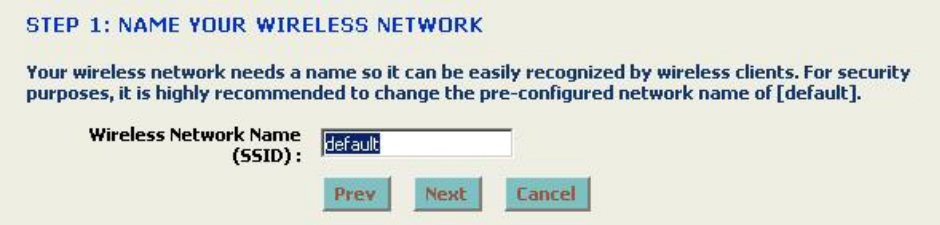
- The connection wizard is complete. Please wait while the system is rebooting.

Note: Do no un-plug the device during this process as this may cause permanent damage.

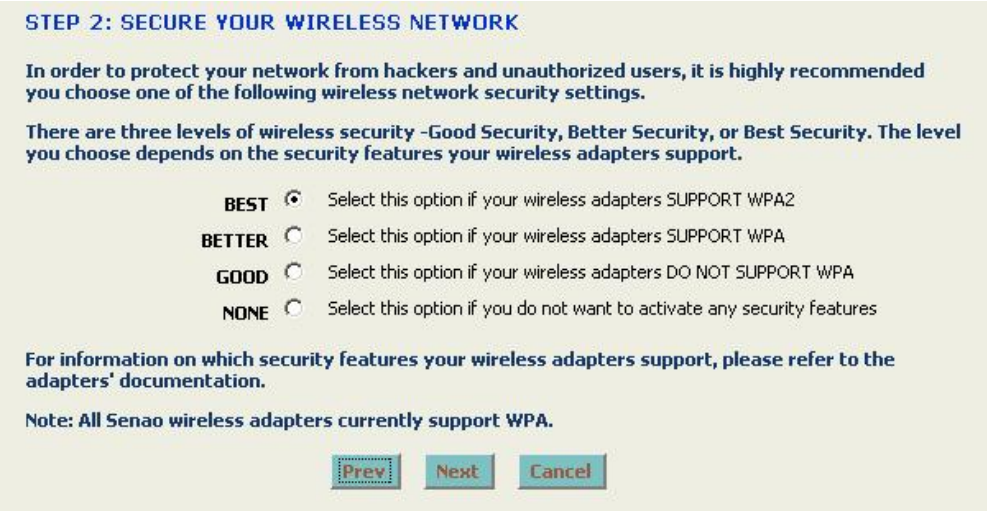
4.2.6.2 Wireless Security Setup Wizard

- The wireless security setup wizard will guide you through the steps to configure the security settings of the device. .
- Click on the **Launch Wireless Security Setup Wizard** button.

- Click on the **Next** button to continue.

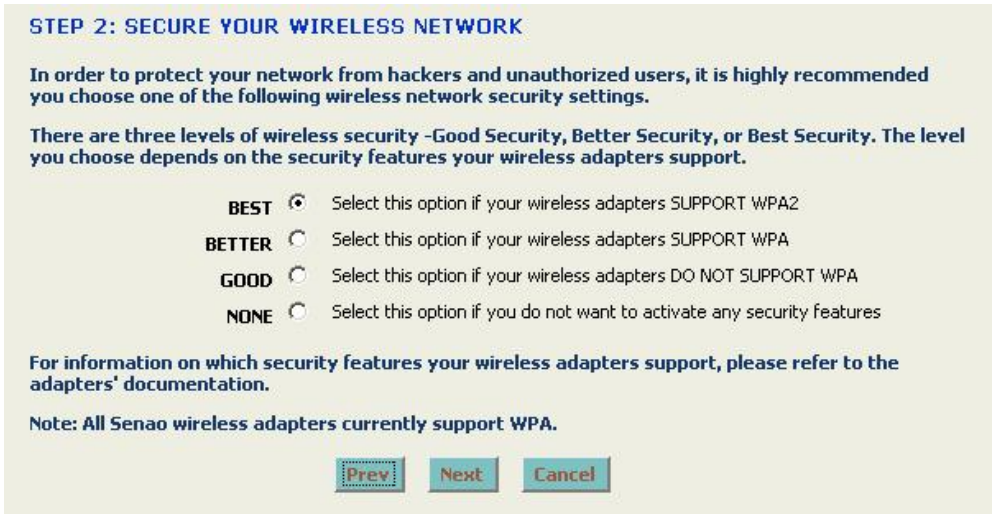


- **Wireless Network Name (SSID)**: The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters.
- Click on the **Next** button to continue.



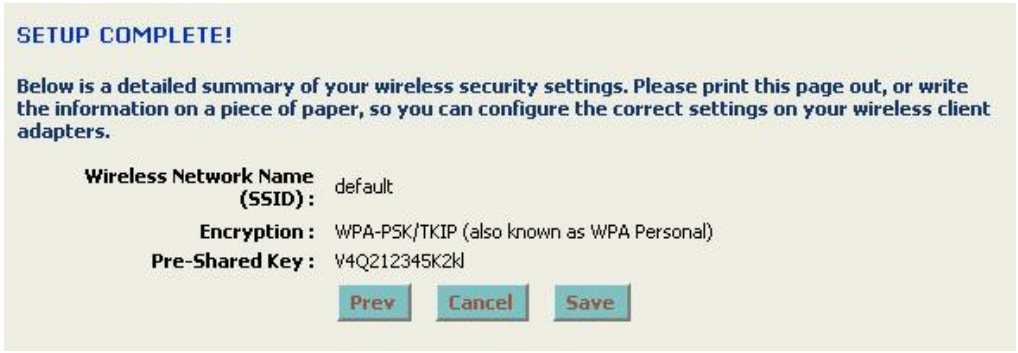
- In order to protect your network from hackers and unauthorized users, it is highly recommended to secure the network using encryption and authentication. Select a level of security and then click on the **Next** button to continue.
- If you do not want to setup security, then select the **NONE** radio button.

4.2.6.2.1 Wireless Security Level: BEST



- Select the **BEST** radio button which supports WPA2 encryption. Then click on the **Next** button.

- Enter a security password between 2 and 20 characters then click on the **Next** button.

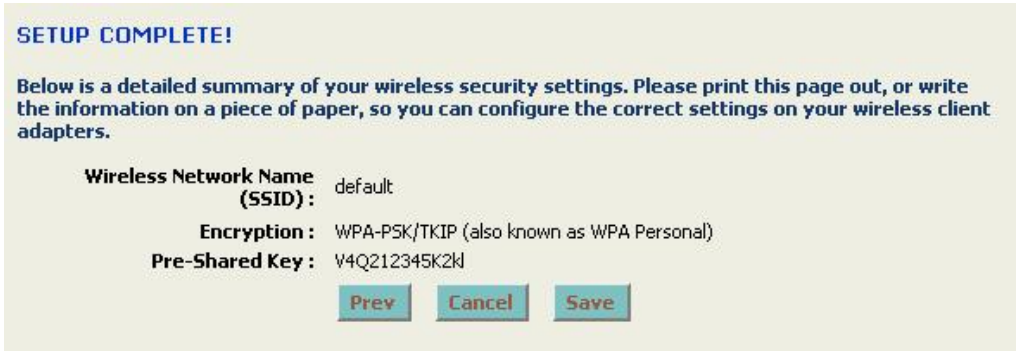


- The setup is complete. Click on the **Save** button and then reboot the device.

4.2.6.2.2 Wireless Security Level: BETTER

- Select the **BETTER** radio button which supports WPA encryption. Then click on the **Next** button.

- Enter a security password between 2 and 20 characters then click on the **Next** button.

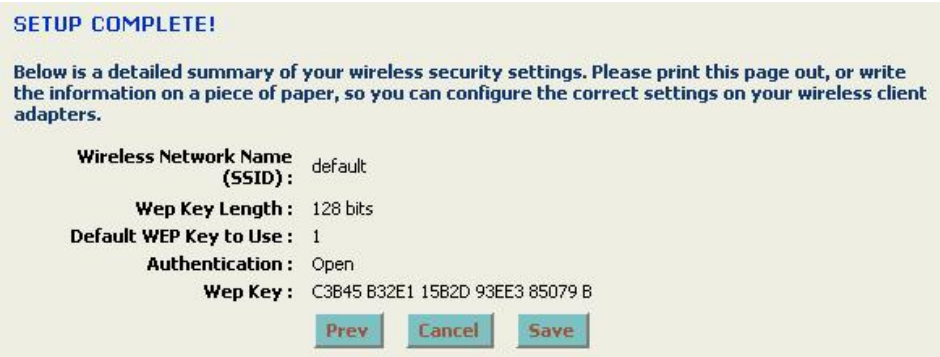


- The setup is complete. Click on the **Save** button and then reboot the device.

4.2.6.2.3 Wireless Security Level: GOOD

- Select the **GOOD** radio button which supports WPA encryption. Then click on the **Next** button.

- Enter a security password between 2 and 20 characters then click on the **Next** button.



- The setup is complete. Click on the **Save** button and then reboot the device.

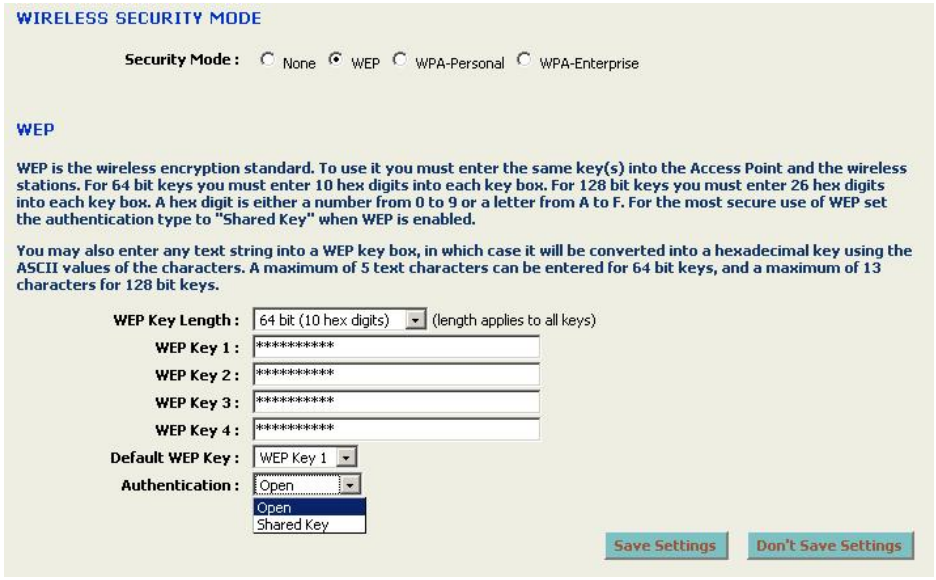
4.3 Wireless Configuration

- Click on the Wireless_11a or Wireless_11g link under the Wireless menu. On these pages you may configure the 802.11a or 802.11g radio.

- **Wireless Network Name**: The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters.
- **Visibility Status**: Select **Visible** or **Invisible**. This is the SSID broadcast feature. If you set this value to Visible, then the clients will be able to find this SSID on a site survey.
- **Channel**: Select a channel from the drop-down list. The channels available are based on the country's regulation. Place a check in the Auto Channel Select box if you would like the Access Point to select the cleanest channel.
- **Transmission Rate**: Select a transmission rate from the drop-down list. It is recommended to use the **Best (automatic)** option.
- **802.11 Mode**: Select the IEEE 802.11 mode from the drop-down list. For example, if you are sure that the wireless network will be using only IEEE 802.11g clients, then it is recommended to select **802.11g** only instead of **Mixed 802.11g and 802.11b** which will reduce the performance of the wireless network. You may also select **802.11b** only or **802.11a only**. Click on the **Save Settings** button once you have modified the settings.

4.3.1.1 WEP (Wired Equivalent Privacy)

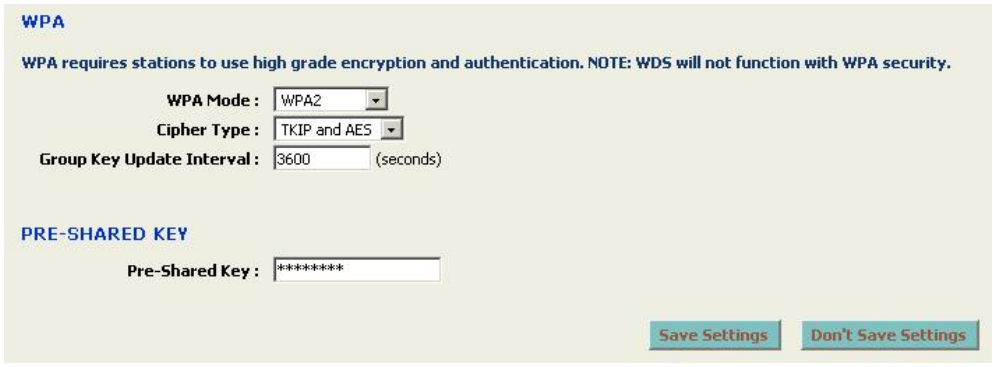
- Select the **WEP** radio button if your wireless network uses WEP encryption. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.
- WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.



- **WEP Key Length**: Select a **64-bit** or **128-bit** WEP key length from the drop-down list.
- **WEP Key 1-4:** You may enter four different WEP keys.
- **Default WEP Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- **Authentication:** Select **Open**, or **Shared Key**. Authentication method from the drop-down list. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.
- Click on the **Save Settings** button once you have modified the settings.

4.3.1.2 WPA Personal (Wi-Fi Protected Access)

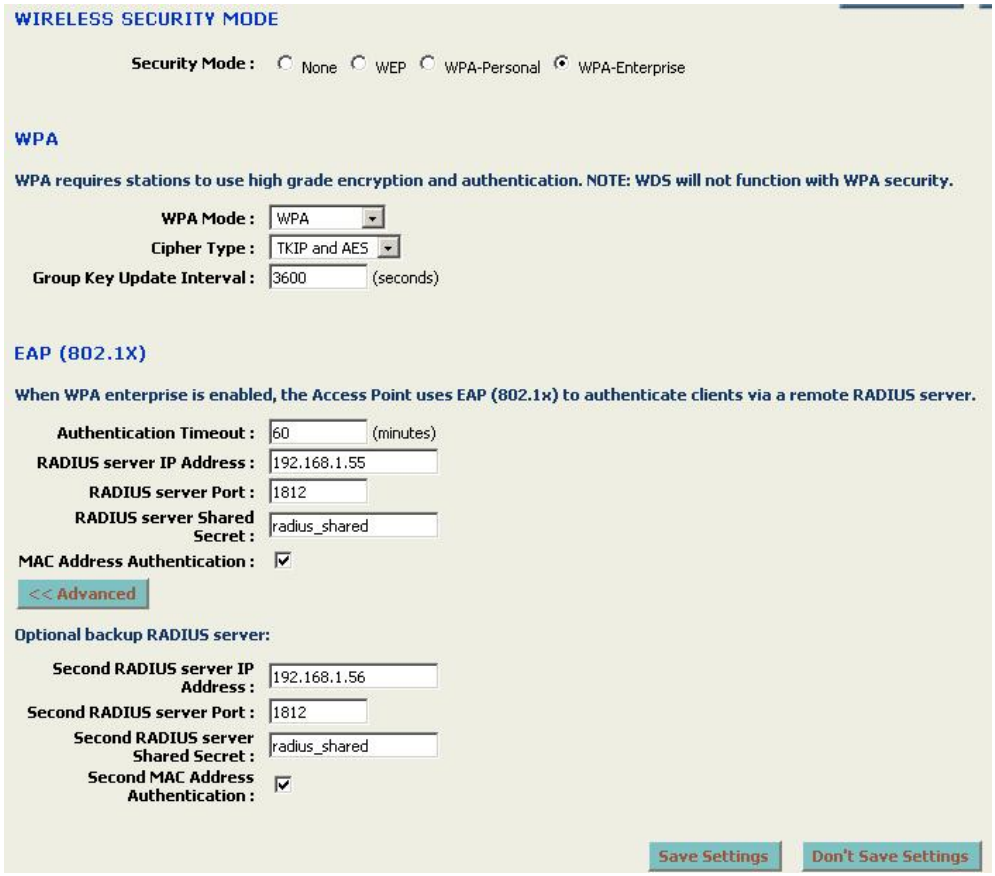
- Select the **WPA-Personal** radio button if your wireless network uses WPA encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.



- **WPA Mode**: Select the WPA / WPA2 from the drop-down list.
- **Cipher Type**: Select TKIP or AES as the cipher suite. The encryption algorithm used to secure the data communication. TKIP. Use TKIP only. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES. Use AES only. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES. TKIP and AES. The bridge negotiates the cipher type with the access point, and uses AES when available.
- **Group Key Update Interval**: Specify the number of seconds before the group key used for broadcast and multicast data is changed.
- **Pre-Shared Key**: The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.
- Click on the **Save Settings** button once you have modified the settings.

4.3.1.3 WPA Enterprise (Wi-Fi Protected Access & 802.1x)

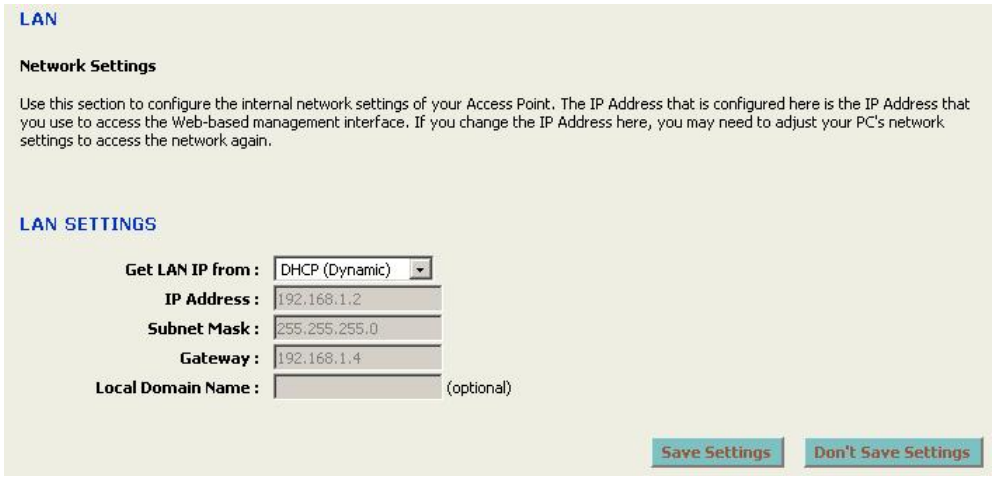
- Select the WPA-Enterprise radio button if your wireless network uses WPA encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.
- This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users.



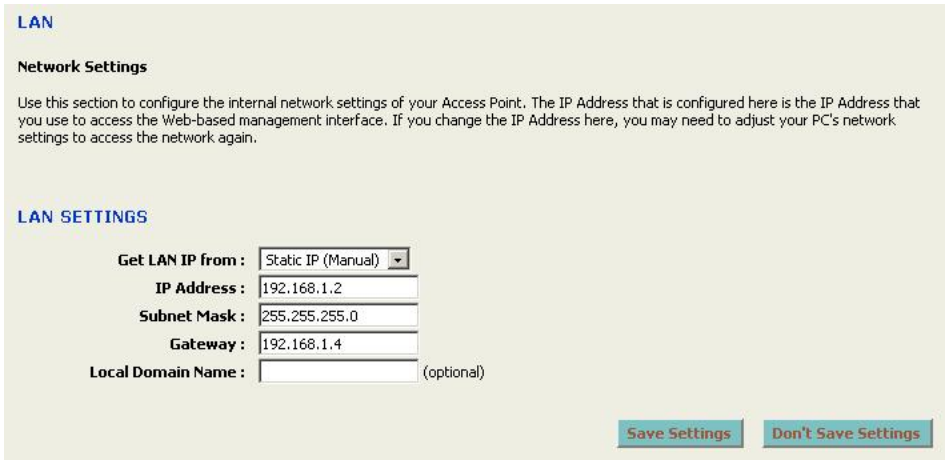
- **WPA Mode**: Select the WPA / WPA2 from the drop-down list.
- **Cipher Type**: Select TKIP or AES as the cipher suite. The encryption algorithm used to secure the data communication. TKIP. Use TKIP only. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES. Use AES only. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES. TKIP and AES. The bridge negotiates the cipher type with the access point, and uses AES when available.
- **Group Key Update Interval**: Specify the number of seconds before the group key used for broadcast and multicast data is changed.
- **Authentication Timeout**: Specify the number of minutes after which the client will be required to re-authenticate.
- **RADIUS Server IP Address**: Specify the IP address of the RADIUS server.
- **RADIUS Server Port**: Specify the port number of the RADIUS server, the default port is 1812.
- **RADIUS Server Shared Secret**: Specify the pass-phrase that is matched on the RADIUS Server.
- **MAC Address Authentication:** Place a check in this box if you would like the user to always authenticate using the same computer.
- Optional Backup RADIUS server: This option enables configuration of an optional second RADIUS server. A second RADIUS server can be used as backup for the primary RADIUS server. The second RADIUS server is consulted only when the primary server is not available or not responding.
- Click on the **Save Settings** button once you have modified the settings.

4.4 LAN

- Click on the **LAN** link under the **LAN** menu. This feature allows you to configure the LAN interface using a static IP address or as a DHCP client/server. This IP address is also used to access the web-based interface.



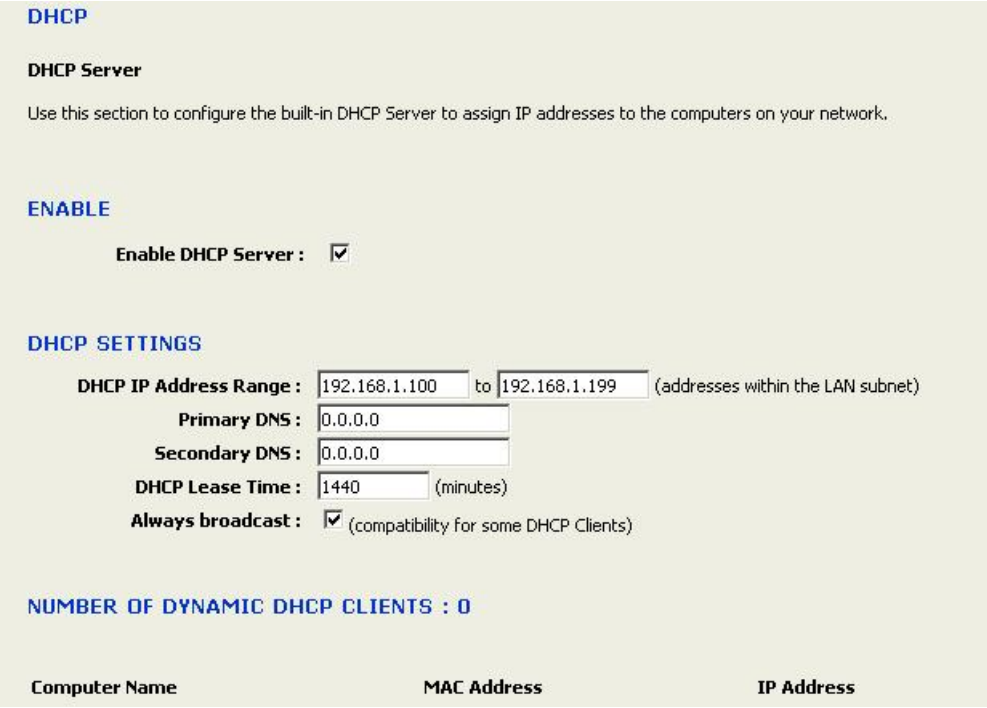
- **Get LAN IP from**: Select **Static IP (Manual)** or **DHCP (Dynamic)** from the drop down list. Choose **DHCP (Dynamic)** if your router supports DHCP and you want the router to assign an IP address to this device. In this case, you do not need to fill in the following fields. Choose **Static IP (Manual)** if your router does not support DHCP or if for any other reason you need to assign a fixed address to this device.
  Note: You cannot choose DHCP (Dynamic) if you have enabled the DHCP Server option on the DHCP page; this device cannot be both a DHCP client and a DHCP server.



- **IP Address:** Enter an IP address for this device.
- **Subnet Mask:** Enter the subnet mask for this IP address.
- **Gateway:** Enter the IP address of the default gateway.
- **Local Domain Name:** Enter a local domain name. This field is optional.
- Click on the **Save Settings** button once you have modified the settings.
  Note: If you change the IP address here, you may need to adjust your PC's network settings to access the network again.

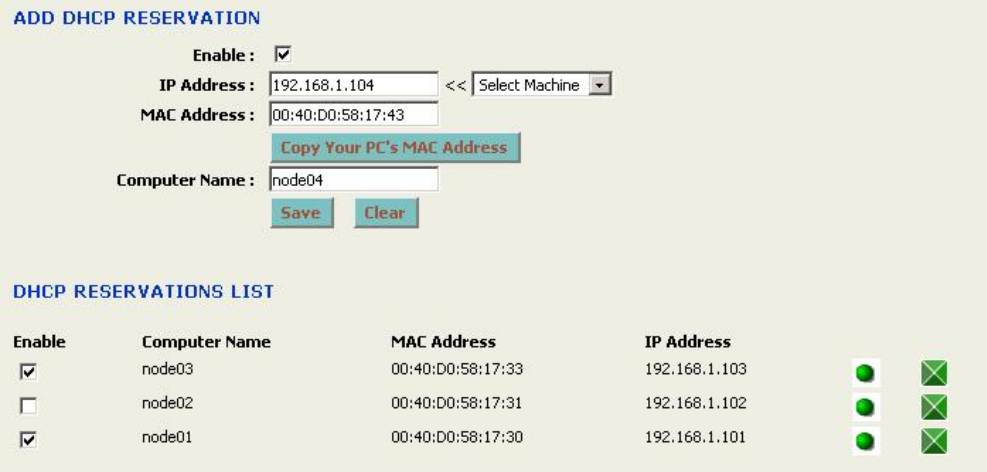
4.5 DHCP Server

- Click on the **DHCP** link under the **LAN** menu. DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN). In most situations, the router provides DHCP services, and you can leave this option disabled. However, if for any reason the router does not provide DHCP services, enable this option. The AP's DHCP Server will then manage the IP addresses and other network configuration information for wireless clients associated with the AP. The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to **DHCP** or **Obtain an IP address automatically**.



- **Enable DHCP Server:** Place a check in this box if you would like this device to function as a DHCP Server.
- **DHCP IP Address Range**: Enter the first and last IP address of the range. Make sure that the range is on the same subnet as the device. These two IP values (from and to) define a range of IP addresses that the DHCP Server uses when assigning addresses to computers and devices on your Local Area Network. Any addresses that are outside of this range are not managed by the DHCP Server; these could, therefore, be used for manually configured devices or devices that cannot use DHCP to obtain network address details automatically.
- **Primary / Secondary DNS:** Enter an IP address for the primary and secondary DNS servers. This field is optional.
- **DHCP Lease Time:** The amount of time that a computer may have an IP address before it is required to renew the lease. The lease functions just as a lease on an apartment would. The initial lease designates the amount of time before the lease expires. If the tenant wishes to retain the address when the lease is expired then a new lease is established. If the lease expires and the address is no longer needed than another tenant may use the address.

- **Always Broadcast:** If all the computers on the LAN successfully obtain their IP addresses from the Access Point's DHCP server as expected, this option can remain disabled. However, if one of the computers on the LAN fails to obtain an IP address from the Access Point's DHCP server, it may have an old DHCP client that incorrectly turns off the broadcast flag of DHCP packets. Enabling this option will cause the Access Point to always broadcast its responses to all clients, thereby working around the problem, at the cost of increased broadcast traffic on the LAN.
- Click on the **Save Settings** button once you have modified the settings.



- **Enable DHCP Reservation:** You may use this feature to reserve a specific IP address for a specific MAC address (node). Place a check in this box to enable this feature.
- **IP Address:** Specify the IP address
- **MAC Address:** Specify the MAC address of the node which will used the reserved IP address.
- **Copy your PCs MAC address:** Click on this button if you would like to reserve an IP address for the PC you are logged on to.
- **Computer Name:** Specify a name for the specified IP address.
- Click on the **Save** button to insert the entry into the DHCP reservations list.

4.6 MAC Address Filter

- Click on the **MAC Address Filter** link under the **Filter** menu. The MAC address filter section can be used to filter network access by machines based on the unique MAC addresses of their network adapter(s). It is most useful to prevent unauthorized wireless devices from connecting to your network. A MAC address is a unique ID assigned by the manufacturer of the network adapter.

- **Enable MAC Address Filter:** You may use this feature to filter the wired and wireless clients. Place a check in this box to enable this feature.
- **Mode**: Select a filter setting from the drop-down list. When **only allow listed machines** is selected, only computers with MAC addresses listed in the MAC Address List are granted network access. When **only deny listed machines** is selected, any computer with a MAC address listed in the MAC Address List is refused access to the network.
- **Filter Wireless Clients**: Place a check in this box if you would like to filter wireless clients.
- **Filter Wired Clients**: Place a check in this box if you would like to filter wired clients.
- **MAC Address:** Specify the MAC address of the node which you would like to filter.
- **Copy your PCs MAC address:** Click on this button if you would like to filter the MAC address for the PC you are logged on to.
- **Computer Name:** Specify a name for the specified MAC address.
- Click on the **Save** button to insert the entry into the MAC address list.

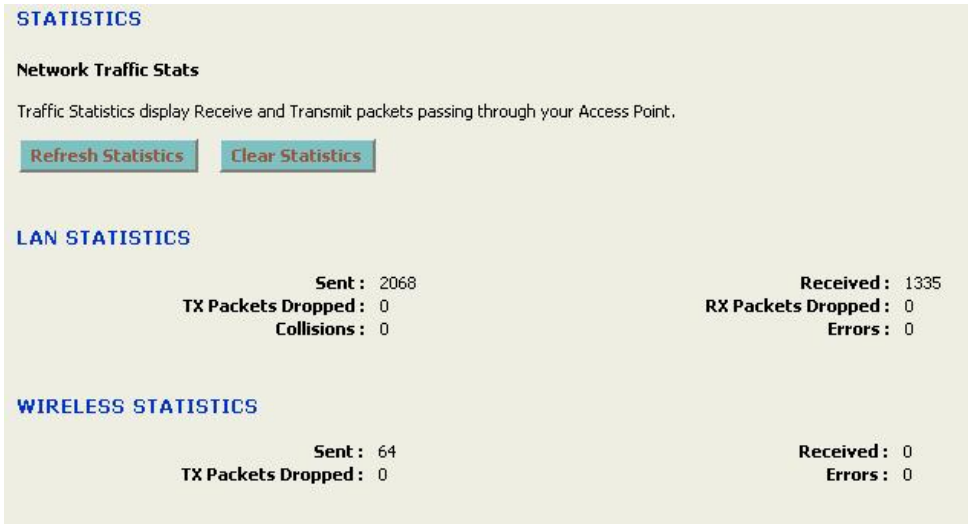
4.7 Logs

- Click on the **Logs** link on the navigation menu. Logs display a list of events that are triggered on the Ethernet and Wireless interface. This log can be referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.

- **Log Options:** Select the type of warning that you would like recorded and place a check in the appropriate box. Then click on the **Apply Log Settings Now** button.
- **Log Details**: The events are logged in this section. Click on the **Refresh** button to refresh the events or click on the **Clear** button to clear the events. Click on the **Save Log** button to save the log on your PC.

4.8 Statistics

- Click on the **Statistics** link on the navigation menu. This page displays the transmitted and received packet statistics of the wired and wireless interface.



- **Sent**: The number of packets sent from the bridge.
- **Received**: The number of packets received by the bridge.
- **TX Packets Dropped**: The number of packets that were dropped while being sent, due to errors, collisions, or bridge resource limitations.
- **RX Packets Dropped**: The number of packets that were dropped while being received, due to errors, collisions, or bridge resource limitations.
- **Collisions**: The number of packets that were dropped due to Ethernet collisions (two or more devices attempting to use an Ethernet circuit at the same time).
- **Errors**: The number of transmission failures that cause loss of a packet. A noisy radio-frequency environment can cause a high error rate on the wireless LAN.
- Click on the **Refresh Statistics** button to refresh the events or click on the **Clear Statistics** button to clear the events.

Appendix A – Specifications

Data Rates

1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps

Standards

IEEE802.11a/b/g, IEEE802.3, IEEE802.3u, IEEE802.3af, IEEE802.1f, IEEE802.1x

Compatibility

IEEE 802.11g/ IEEE 802.11b

Power Requirements

Active Ethernet (Power over Ethernet) –48 VDC/0.375A

External Unit: Auto sensing 100/240 VAC; 50/60 Hz

Regulation Certifications

FCC Part 15/UL, ETSI 300/328/CE

RF Information

Frequency Band

802.11a: 5.15~5.25GHz, 5.25~5.35GHz, 5.47~5.725GHz, 5.725~5.825GHz

802.11b/g: U.S., Europe and Japan product covering 2.4 to 2.484 GHz, programmable for different country regulations

Media Access Protocol

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Modulation Technology

Orthogonal Frequency Division Multiplexing (OFDM)
DBPSK @ 1Mbps
DQPSK @2Mbps
CCK @ 5.5 & 11Mbps
BPSK @ 6 and 9 Mbps
QPSK @ 12 and 18 Mbps
16-QAM @ 24 and 36 Mbps
64-QAM @ 48 and 54 Mbps

Operating Channels

802.11b/g:
11 for North America, 14 for Japan, 13 for Europe,
802.11a:

US/Canada:12 non-overlapping channel (5.15~5.35GHz, 5.725~5.825GHz)

Europe:19 non-overlapping channel (5.15~5.35GHz, 5.47~5.825GHz)

Japan: 4 non-overlapping channel (5.15~5.25GHz)

China: 5 non-overlapping channel (5.725~5.85GHz)

Receive Sensitivity (Typical)

- 5.15~5.85G(IEEE802.11a)

6Mbps@ -88dBm;
54Mbps@ -70dBm

- 2.412~2.472G(IEEE802.11g)

6Mbps@ -91dBm;
54Mbps@ -74dBm

- 2.412~2.472G(IEEE802.11b)

11Mbps@ -90dBm

1Mbps@ -95dBm

Available transmit power (Typical)

- 5.15~5.24 GHz(IEEE802.11a)

17dBm @6 ~ 24Mbps
17dBm @36Mbps
16 dBm @48Mbps
15 dBm @54Mbps

- 5.26~5.35GHz(IEEE802.11a)

20dBm @6 ~ 24Mbps
18dBm @36Mbps
16 dBm @48Mbps
15 dBm @54Mbps

- 5.745~5.85GHz (IEEE802.11a)

18dBm @6 ~ 24Mbps
16dBm @36Mbps
14 dBm @48Mbps
13 dBm @54Mbps

- 2.412~2.472G(IEEE802.11g)

26dBm @6 ~ 24Mbps
23dBm @36Mbps
22 dBm @48Mbps
21 dBm @54Mbps

- 2.412~2.472G(IEEE802.11b)

up to 26 dBm. @1, 2, 5.5 and 11Mbps

RF Connector

SMA (Fr) Type

Networking

Topology

Ad-Hoc, Infrastructure

Operation Mode

Point-to-Point/ Point-to-Multipoint Bridge/ AP/ Client Bridge/ WDS

Interface

Wireless IEEE802.11b/g

One 10/100 RJ-45 port

Security

- IEEE802.1x Authenticator / RADIUS Client (EAP-MD5/TLS/TTLS) Support in AP Mode
- WPA/WPA2 Supplicant support in Client Bridge Mode
- WPA /WPA2/ Pre Share KEY (PSK) with TKIP/AES
- MAC address filtering (AP only)
- Hide SSID in beacons

IP Auto-configuration

DHCP client/server

Management

Configuration

Web-based configuration (HTTP)
Telnet Configuration
SNMP V1

Firmware Upgrade

Upgrade firmware via web-browser
Serial Interface (RS-232)
TFTP

Physical

Dimensions (HxWxD)

163.8(L)mm * 135.2(W)mm * 47.0(H)mm

Weight

1.2 Kg (2.6 lbs)

Environment

Temperature Range

Operating: -20°C to 60°
Storage: -40°Cto 80°

Humidity (non-condensing)

5%~95% Typical

Appendix B – FCC Interference Statement

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

We declare that the product is limited in CH1~CH11 by specified firmware controlled in the USA.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IC statement

Operation is subject to the following two conditions:
This device may not cause interference and
This device must accept any interference, including interference that may cause undesired operation of the device.
This device has been designed to operate with an antenna having a maximum gain of 9 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

IMPORTANT NOTE:
IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Règlement d'Industry Canada

Les conditions de fonctionnement sont sujettes à deux conditions:
Ce périphérique ne doit pas causer d'interférence et.
Ce périphérique doit accepter toute interférence, y compris les interférences pouvant perturber le bon fonctionnement de ce périphérique.